



ECKINGTON SCHOOL SAFEGUARDING POLICY

Policy Author	Trust Designated Safeguarding Lead
Date Last Reviewed	September 2021
Trust Key Reader	KB
Approved by Trust Board	09.09.21
Review Date	September 2022

LEAP MAT

Eckington Safeguarding Policy incorporating Child Protection: Keeping Children Safe in Education

Policy Consultation & Review

LEAP MAT has an overarching safeguarding policy incorporating child protection which each Academy within the Trust then builds upon to ensure locally agreed multi-agency safeguarding arrangements by the three safeguarding partners are implemented (as advised within Keeping Children Safe in Education (KCSE) 2021).

Each school within LEAP MAT uses an overarching LEAP policy but then personalises it and has their own bespoke policy on their individual website; copies are also available on request from the each school office. We also inform parents and carers about this policy when their children join each academy and through each academy's newsletter.

Within each Academy, their bespoke policy is provided to all staff (including temporary staff and volunteers) at induction alongside our Staff Code of Conduct and Behaviour Policy. In addition, all members of staff are provided with Part One of the statutory guidance 'Keeping Children Safe in Education', DfE, 2021 (KCSE) and are made aware of the role of the designated safeguarding team, as well as everyone's responsibility for monitoring attendance to help prevent children missing from education.

Our policy will be reviewed in full by the Board of Trustees on an annual basis.

The policy was updated September 2021 in light of new statutory guidance, Keeping Children Safe in Education 2021 and the latest government guidance linked to COVID-19 and safeguarding and school opening. It is anticipated that Annex 4 (policy addendum linked to COVID-19) in particular will be updated throughout the year if new guidance comes into effect or should there be a local/ national lockdown.

Page:	
3	Purpose & Aims
6	Ethos & Teaching
8	Roles & Responsibilities
11	Training & Induction
12	Procedures for Managing Concerns
15	Recording & Information Sharing
16	Working with Parents & Carers
16	Child Protection Conferences
17	Safer Recruitment
20	Safer Working Practice
21	Managing Allegations against Staff
24	Child on Child Sexual Violence and Sexual Harassment
31	e-Safeguarding- using technology
45	Other relevant policies
45	Statutory Framework
46	Making a referral (Appendix 1)
48	Categories of abuse (Appendix 2)
52	Further information (Appendix 3)
62	COVID-19: school closure safeguarding arrangements (Appendix 4)
69	Internet setting (Appendix 5)
72	Acceptable Use polices (Appendix 6)

1. PURPOSE & AIMS

- 1.1 The purpose of LEAP Multi-Academy Trust (Brinsworth Academy, Dinnington High School and Eckington School) safeguarding policy is to ensure every child who is a registered student at one of our Academies is safe and protected from harm. This means we will always work to:-
- Protect children and young people at our Academies from maltreatment
 - Prevent impairment of our children's **mental and physical** health or development
 - Ensure that children and young people at our Academies grow up in circumstances consistent with the provision of safe and effective care
 - Undertake that role so as to enable children and young people at our Academies to have the best outcomes.
- 1.2 This policy gives clear direction to staff, volunteers, visitors and parents/carers about expected behaviour and our legal responsibility to safeguard and promote the welfare of all students at our Academies.
- 1.3 Our Academies fully recognise the contribution they make to protect children from harm and supporting and promoting the welfare of all children who are registered students at our Academies. This will also include identifying children who may benefit from early help. The elements of our policy are **prevention, protection and support**.
- 1.4 This policy applies to all students, staff, parents/carers, Governors, Trustees, volunteers and visitors. The policy should be read in conjunction with other LEAP policies notably Staff Safeguarding Code of Conduct, Behaviour policy, Staff and Student Acceptable Use Agreements, Information Technology Security Document, GDPR Data Protection Policy, GDPR working practices document, Anti-Bullying Policy and the Searching and Screening policy.
- 1.5 This policy recognises the COVID-19 safeguarding advice for schools as outlined in Appendix 4; it makes particular reference to school re-opening and closures and it is this section of the policy that will more than likely be updated throughout the coming months in response to any government guidance regarding future closures and blended learning).
- 1.6 This policy includes online safeguarding throughout with sections 13-28 focusing on technology and its use in school.

What is Abuse?

- 1.7 **All staff** should be aware of indicators of abuse and neglect so that they are able to identify cases of children who may be in need of help or protection and those who would benefit from **early help**. **All staff** should be aware that safeguarding **incidents and/or behaviours can be associated with factors outside the school** and/or can occur between children outside of these environments (**contextual safeguarding**).
- Abuse may fall into a number of categories: - **physical abuse, sexual abuse, emotional abuse and neglect**. Abuse and neglect are forms of maltreatment of a child. Somebody may abuse or neglect a child by inflicting harm or by failing to act to prevent harm. Children may be abused in a family or in an institutional or community setting, by those known to them or, more rarely, by a stranger. They may be abused by an adult or adults, or another child or children (this is known as **peer-on-peer abuse and it is important**

staff know how we will deal with this in school – see section 12). (See Appendix 2 for more detailed definitions).

- Staff should be mindful of the **use of technology** as online abuse can take place concurrently. Children can also abuse peers online eg harassment, misogynistic messages, non-consensual sharing of indecent images, sharing abusive images, pornography.
- All staff should have an awareness of safeguarding issues that can put children at risk of harm. Behaviours linked to issues such as drug taking, alcohol abuse, deliberately missing education and sending, sharing, receiving sexual images (nudes/ semi-nudes) put children in danger. It is important to recognise that **extra-familial** (outside the family) harms can take a variety of forms e.g. CSE CCE and staff need to be aware of such risks.
- Where staff are unsure, they should always speak to the Designated Safeguarding Lead (DSL).
- **Child sexual exploitation (CSE) and Child Criminal Exploitation (CCE)**
 - KCSE makes particular reference to these 2 types of abuse and this emphasises the importance that ALL staff are aware of the signs and indicators of such abuse where an individual or group takes advantage of **an imbalance in power to coerce, manipulate or deceive a child into sexual or criminal activity in exchange for something the victim needs or wants and /or for the financial advantage or increased status of the perpetrator**. The experience of girls exploited may be different to those of boys; the indicators of CCE may also differ. Risk factors which increase the likelihood of involvement in **serious violence** include, being male, frequent absence from school, previous involvement in offending and having experienced child maltreatment. More information include definitions and indicators are included in Appendix 2.
- **Domestic abuse:** ALL staff need to be aware that domestic abuse is: any incident or pattern of incidents of controlling, coercive, threatening behaviour, violence or abuse between those aged 16 or over who are, or have been, intimate partners or family members regardless of gender or sexuality.

The abuse can encompass, but is not limited to: psychological; physical; sexual; financial; and emotional.

All children can witness and be adversely affected by domestic abuse in the context of their home life where domestic abuse occurs between family members. Exposure to domestic abuse and/or violence can have a serious, long lasting emotional and psychological impact on children. In some cases, a child may blame themselves for the abuse or may have had to leave the family home as a result.

Our school is part of **Operation Encompass**, where we receive alerts from the police where children have been present/live in the household where there has been an domestic abuse incident; staff of that child are alerted to monitor closely and report concerns to the safeguarding /pastoral teams so that we can best support the student (see section 6.4).

Peer on peer abuse (child on child)

- All staff should be aware that children can abuse other children (often referred to as peer on peer abuse). And that it can happen both inside and outside of school and online. It is important that all staff recognise that girls are more likely to be victims and boys' perpetrators, but all peer on peer abuse is unacceptable and will be taken seriously. The indicators and signs of peer on peer abuse can vary between girls and boys and it is important that staff know how to identify abuse and respond to reports.
- **As a staff, we recognise that that even if there are no reports of peer on peer harassment and abuse, it does not mean it is not happening, it may be the case that it is just not being reported.** As such it is important if staff have any concerns regarding peer on peer abuse they should respond to these and inform the designated safeguarding lead /team.
- **It is the important that all staff challenge inappropriate behaviours between peers**, many of which are listed below, that are actually abusive in nature. Downplaying certain behaviours, for example dismissing sexual harassment as "just banter", "just having a laugh" or "part of growing up" creates a culture that normalises abuse leading to children accepting it as normal and not coming forward to report it. It is therefore vital to have a **zero-tolerance approach** to abuse.
- Peer on peer abuse can include a range of behaviours such as bullying; abuse in intimate personal relationships between peers; physical abuse such as hitting, shaking; sexual violence, such as rape; sexual harassment, such as sexual comments, remarks, jokes and online sexual harassment; consensual and non-consensual sharing of nudes and semi nudes' images; upskirting; initiation/hazing type violence and rituals. All of these examples could also involve an online element too. See Appendix 2 for further details.
- Section 12 of our policy will also explore this issue in greater depth.

Mental Health

- The inclusion in the safeguarding definition, KCSE (para 4), to include mental and physical health, clearly indicates the importance of being aware of the impact of mental health within safeguarding.
- All staff should also be aware that mental health problems can, in some cases, be an indicator that a child has suffered or is at risk of suffering abuse, neglect or exploitation.
- However, whilst, it should be noted that only appropriately trained professionals should attempt to make a diagnosis of a mental health problem, **staff are well placed to observe children day-to-day and identify those whose behaviour suggests that they may be experiencing a mental health problem or be at risk of developing one.** Where staff have concerns, these should be passed on using our established safeguarding procedures.
- Additional guidance on these safeguarding issues as well as issues such as Honour Based Violence, Female Genital Mutilation, Forced Marriage Domestic Abuse, Peer on Peer abuse, Sexual Harassment and Violence, Upskirting, Child Criminal Exploitation, Children and Court System, Family Members in Prison, Preventing Radicalisation and peer on per abuse can be found in Appendix 2 and Appendix 3. Information about the indicators of

abuse is also found in Rotherham Local Safeguarding Children's Partnerships procedures <https://rotherhamsccb.proceduresonline.com/>

- Where children have suffered abuse and neglect, or other potentially traumatic **adverse childhood experiences (ACEs)**, this can have a lasting impact throughout childhood, adolescence and into adulthood. It is key that staff are aware of how these children's experiences, can impact on their mental health, behaviour and education (see Appendix 2 for further information).
 - It is important to recognise that as we return to full school opening, we need to be particularly mindful of student and staff well-being – that people will react differently and we will need to support over time (see Appendix 4 for further information).
 - Staff should refer to the Staff Planner for a summary of signs and indications of abuse, with further details in KCSE paragraphs 19-40. Staff should be particularly aware of vulnerable groups of students including
 - Students with SEND*
 - Students with mental health issues*
 - Young carers
 - Students drawn into antisocial/criminal behaviour
 - Students who frequently go missing and/or persistently absent for part of the day *
 - Looked after children, returning from care, privately fostered, previously looked after*
 - Students misusing drugs/alcohol
 - Students at risk of modern slavery, trafficking or exploitation, radicalisation
 - Students at risk of honour-based abuse such as Female Genital Mutilation(FGM), Forced Marriage
 - Students living in challenging family situations
 - Students showing early signs of abuse and/or neglect
- *See section 5 for more details

Early Help and Support for Children In need

- Early Help means providing support as soon as a problem emerges, at any point in a child's life, from the foundation years through to the teenage years. We will work with local agencies in Derbyshire/Sheffield to put processes in place for the effective assessment of the needs of individual children who may benefit from early help services. We will monitor and review cases and 'step up' should the child's situation not appear to be improving or is getting worse. We understand the importance of contextual safeguarding and looking at harm outside of the home.

2. OUR ETHOS

- 2.1 **Safeguarding and promoting the welfare of children is everyone's responsibility (KCSE para 2, 82) and as such safeguarding underpins all of our work.** The child's welfare is of paramount importance. Our Academy will establish and maintain an ethos where students feel secure, are encouraged to talk, are listened to and are safe. Children at our Academy will be able to talk freely to any member of staff if they are worried or concerned about something and their **wishes and feelings** will be taken into account when determining action. Student planners give advice about our safeguarding team as well as signposting to help

beyond school. We are also developing posters with student focus groups to advertise how to report concerns in school to increase awareness and reassure students that they will be taken seriously.

All staff should be able to reassure victims that they are being taken seriously and that they will be supported and kept safe. A victim should never be given the impression that they are creating a problem by reporting abuse, sexual violence or sexual harassment. Nor should a victim ever be made to feel ashamed for making a report.

2.2 **Everyone who comes into contact with children and their families has a role to play in safeguarding children.** We recognise that all staff in our Academy play a particularly important role as they are in a position to identify concerns early and provide help for children to prevent concerns from escalating. **All staff are advised to maintain an attitude of ‘it could happen here’ where safeguarding is concerned.** The best interests of the child must be at the centre of everything we do. This is particularly true when thinking about sexual harassment and online sexual harm: all staff must assume our students experience such behaviours and this be a basis of our work pastorally and within the curriculum.

2.3 All staff and regular visitors will, through training and induction, know how to recognise indicators of concern, how to respond to a disclosure from a child and how to record and report this information. We will not make promises to any child and we will not keep secrets. Every child will know what the adult will have to do with any information they have chosen to disclose.

2.4 Throughout our curriculum we will provide activities and opportunities for children to develop the skills they need to identify risks and stay safe. This will also be extended to include material that will encourage our children to develop essential life skills. Our curriculum lessons along with our morning guidance provision with form tutors play a significant role in raising awareness with students about how to stay safe, including e-safeguarding. We use outside agencies and theatre in education events to complement the work of staff around issues such as CSE/grooming, domestic violence and positive relationships.

2.5 At all times we will work in partnership and endeavour to establish effective working relationships with parents, carers and colleagues from other agencies in line with Working Together to Safeguard Children (2018).

Link:

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/729914/Working Together to Safeguard Children-2018.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/729914/Working_Together_to_Safeguard_Children-2018.pdf)

2.6 OPPORTUNITIES TO TEACH SAFEGUARDING

As part of our broad and balanced curriculum we believe that it is important to teach safeguarding, including online safety and use our Character curriculum for much of this along with our ICT based courses. Within the Character curriculum is included the statutory Relationships and Sex Education (RSE), Health Education as well as work around British Values and Careers preparation). Staff can also visit the following for further advice about teaching RSE. <https://www.gov.uk/guidance/teaching-about-relationships-sex-and-health>.

Online safety and remote teaching – please refer to the safeguarding addendum (Appendix 4) for guidance about staff conduct and procedures for online learning and teaching. See also the LEAP Safeguarding Staff Code of Conduct. We also use UKCIS resources to help create our online safety curriculum.

All our **Personal Development** work, supports our safeguarding work as we use all interactions, including tutor time, assemblies and all lessons to reinforce the importance of respectful and healthy relationships in all aspects of life. Our strong pastoral system plays a key role in this.

3. ROLES AND RESPONSIBILITIES

Role	Name	Contact details
Eckington School Designated Safeguarding Lead (DSL)	Mrs A Burgess	alison.burgess@eck.leaptrust.co.uk
Named Safeguarding Governor	Mrs Wormleighton J	Jill.wormleighton@eck.leaptrust.co.uk
Named Safeguarding Trustee	Mrs K Bottomley	info@leap-mat.org.uk

- 3.1 It is the responsibility of **every** member of staff, volunteer and regular visitor to our Academy to ensure that they carry out the requirements of this policy and, at all times, work in a way that will safeguard and promote the welfare of all of the students at Eckington School. This includes the responsibility to provide a safe environment in which students can learn.

The Board of Trustees and Local Governing Bodies

- 3.2 The Board of Trustees is accountable for ensuring the effectiveness of this policy and our compliance with it. Although our Board of Trustees takes collective responsibility to safeguard and promote the welfare of our students, we also have a named Trustee who champions safeguarding within the Multi-Academy Trust. Within each local governing body, there is a named safeguarding governor who works with the Designated Safeguarding Lead (DSL) and also the named Trustee.
- 3.3 The Board of Trustees will ensure that:-
- The safeguarding policy is in place and is reviewed annually, is available publicly via our Academy website and has been written in line with Local Authority guidance and the requirements of Derbyshire Local Safeguarding Partnership policies and procedures.
 - Each Academy in this Trust contributes to inter-agency working in line with Working Together to Safeguard Children (2018), updated December 2020. In Derbyshire, a termly **DSL Forum** is a collective mechanism for engaging with the 3 safeguarding partners in the borough. The school regularly meets with the Early Help Locality manager as part of a wider safeguarding team to support students and families in our local area.
 - Each Academy has due regard to the **Prevent Duty** Guidance 2015, under Section 26 of the Counter-Terrorism and Security Act 2015, which aims to prevent children and young people from being drawn into extremism and terrorism. This may include making a referral to the **Channel** programme which provides a mechanism for schools to make referrals via Derbyshire Starting Point if they are concerned that an individual might be vulnerable to

radicalisation (see Appendix A for further details on Preventing radicalisation, Prevent Duty and Channel and additional information about terrorism).

- Each Academy has due regard to the **mandatory** reporting duty, which came into force in October 2015, of the **Female Genital Mutilation** Act 2003 which places a **statutory duty** on teachers (along with social workers and healthcare professionals) to report to the police where they discover that FGM appears to have been carried out on a girl under 18 years (see Appendix 3 for further details on Honour based violence and FGM).
 - A member of the senior leadership team in each Academy is designated to take the lead responsibility for safeguarding and child protection and that there is an alternate and appropriately trained member of staff identified to deal with any issues in the absence of the designated safeguarding lead professional. **There will always be cover for this role.**
 - All staff receive a safeguarding induction and are provided with a copy of this policy, Part One of 'Keeping children safe in Education', the staff safeguarding code of conduct and Behaviour Policy.
 - All staff undertake appropriate safeguarding and child protection training that is updated regularly; in addition, all staff members will receive safeguarding and child protection updates (for example, via e-mail, e-bulletins and staff meetings), as required, but at least annually, to provide them with relevant skills and knowledge to safeguard children effectively.
 - Procedures are in place for dealing with allegations against members of staff, including supply staff (who although not directly employed by the school, the school will take a leading role in following through the allegations and volunteers in line with statutory guidance.
 - Safer recruitment practices are followed in accordance with the requirements of 'Keeping Children Safe in Education' DfE (2021) and also Derbyshire's safeguarding procedures. (<https://schoolsnet.derbyshire.gov.uk>). Our safer recruitment procedures are outlined in the LEAP Trust Safer Recruitment procedures document.
 - They remedy without delay any weakness in regard to our safeguarding arrangements that are brought to their attention.
- 3.4 The Board of Trustees/Governors will receive a safeguarding report at each meeting. It will not identify individual students.

The Principal

- 3.5 Within LEAP Multi-Academy Trust each Principal is responsible for:-
- Identifying a member of the senior leadership team to be the Designated Safeguarding Lead (DSL)
 - Identifying an alternative member of staff to act as the Designated Safeguarding Lead (DSL) in his/her absence to ensure there is always cover for the role
 - Ensuring that the policies and procedures adopted by the Board of Trustees, particularly concerning referrals of cases of suspected abuse and neglect, are followed by all staff
 - Ensuring that all staff and volunteers feel able to raise concerns about poor or unsafe practice and such concerns are addressed sensitively in accordance with agreed whistle-blowing procedures

- Liaise with the LADO for Derbyshire, in the event of an allegation of abuse being made against a member of staff.
- Ensuring that all staff receive relevant training to enable them to carry out their roles, including the appropriate use of ICT
- Reviewing and responding to safeguarding incidents and liaising with the IT support team

The Designated Safeguarding Lead

3.6 The Designated Safeguarding Lead (DSL) will carry out their role in accordance with the responsibilities outlined in Annex B of *'Keeping Children Safe in Education'*. The DSL will work with other senior leaders and take **lead responsibility** for promoting educational outcomes by knowing the welfare, safeguarding and child protection issues that children in need are experiencing, or have experienced, and identifying the impact that these issues might be having on children's attendance, engagement and achievement at school or college' (see KCSE 2021 page 147). This is a new addition to the role and will require key pastoral leads and the SENDCO working closely with the DSL to understand the educational progress and attainment of children who have had/have a social worker and maintaining a culture of high aspirations for this cohort as well as providing additional academic support or reasonable adjustments to help these children meet their potential.

The DSL will provide advice and support to other staff on child welfare and child protection matters.

The role of the designated safeguarding lead carries a significant level of responsibility, and they should be given the additional time, funding, training, resources and support they need to carry out the role effectively.

- 3.7 The DSL/DSL team at each Academy will ensure appropriate representation of the Academy at child protection conferences and core group meetings. Through appropriate training, knowledge and experience our DSL/ DSL team will liaise with Children's Services and other agencies where necessary, and make referrals of suspected abuse to Children's Services, take part in strategy discussions and other interagency meetings and contribute to the assessment of children, including Early Help assessments.
- 3.8 The DSL will maintain written records and child protection files ensuring that they are kept confidential and stored securely through the use of CPOMS.
- 3.9 The DSL is responsible for ensuring that all staff members and volunteers are aware of our policy and the procedure they need to follow. They will ensure that all staff, volunteers and regular visitors have received appropriate child protection information during induction and have been trained to the appropriate level recommended by the local Safeguarding Partnership.
- 3.10 The DSL (and DSL team) complete regular training in line with statutory guidance. In addition, information is shared from local safeguarding forums as well as other safeguarding sources of support.
- 3.11 During term time, the designated safeguarding lead and/or a deputy are available (during school hours) for staff in the school to discuss any safeguarding concerns.

All staff:

3.12 All staff are responsible for implementing safeguarding related policies and reporting any concerns of abuse, neglect or suspected misuse of ICT, using agreed procedures

4. TRAINING & INDUCTION

- 4.1 All staff – will receive regular safeguarding and child protection updates as required, but at least annually, to provide them with relevant skills and knowledge to safeguard children effectively. When new staff, Trustees, Governors, volunteers or regular visitors join our Academies they will be informed of the safeguarding arrangements in place. They will be given a copy/sent an electronic copy of our LEAP safeguarding policy along with the staff safeguarding code of conduct, KCSE Part I and the Behaviour Policy and told who our Designated Safeguarding Lead/Safeguarding team are.
- 4.2 New staff or long-term volunteers will have an induction meeting that will include essential safeguarding information. This programme will include basic safeguarding information relating to signs and symptoms of abuse, how to manage a disclosure from a child, how to record this information and discuss issues of confidentiality. The induction will also remind staff and volunteers of their responsibility to safeguard all children at our Academy and the remit of the role of the Designated Safeguarding Lead.
- 4.3 In addition to the safeguarding induction, all members of staff will undertake appropriate safeguarding training on a regular basis in accordance with '*Keeping Children Safe in Education*' (2021) and advice from the local Safeguarding Partnership. All staff members will also receive regular safeguarding and child protection updates (for example, via e-mail or at staff meetings) as required, but at least annually, to provide them with relevant skills and knowledge to safeguard children effectively. This includes annually completing online training (Hays L1 Safeguarding and child protection).
- 4.4 All regular visitors and volunteers to our Academies will be given a set of our safeguarding procedures; they will be informed of whom our DSL and DSL Team are and what the recording and reporting system is.
- 4.5 The DSL, the DSL team and any other senior member of staff who may be in a position of making referrals or attending child protection conferences or core groups will attend one of the multi-agency training courses organised by Derbyshire Local Safeguarding Partnership/ national charity e.g. NSPCC, at least once every two years. They will also receive regular safeguarding updates throughout the school year in order to keep up with any developments relevant to their role.
- 4.6 Our Board of Trustees/governors will also undertake appropriate training to ensure they are able to carry out their duty to safeguard all of the children at our Academy. Training for Trustees to support them in their safeguarding role is available from Governor Development Service.
- 4.7 We actively encourage all of our staff to keep up to date with the most recent local and national safeguarding advice and guidance. Part One of '*Keeping Children Safe in Education*' (2021) provides links to guidance on specific safeguarding issues such as Child Sexual Exploitation, Honour Based Violence, Children Missing from Education and Preventing Radicalisation, Peer on Peer abuse, Sexual Harassment and Violence, Homelessness, Courts System and Family Members in prison as well as other key areas. In addition, local guidance can be accessed via Derbyshire's Keeping Safe in Education website <https://schoolsnet.derbyshire.gov.uk>. The DSL will also provide regular safeguarding updates for staff.

5. PROCEDURES FOR MANAGING CONCERNS

- 5.1 LEAP Multi-Academy Trust adheres to child protection procedures that have been agreed locally through Derbyshire's Local Safeguarding Partnership.
- 5.2 Every member of staff including volunteers working with students at our schools are advised to maintain an attitude of '*it could happen here*' where safeguarding is concerned. When concerned about the welfare of a child, staff members should always act in the interests of the child and have a responsibility to take action as outlined in this policy.
- 5.3 It is **not** the responsibility of Academy staff to investigate welfare concerns or determine the truth of any disclosure or allegation. **All staff, however, have a duty to recognise concerns and pass the information on in accordance with the procedures outlined in this policy.**
- 5.4 The DSL or DSL team should be used as a first point of contact for concerns and queries regarding any safeguarding concern in our Academy. **Any member of staff or visitor to the Academy who receives a disclosure of abuse or suspects that a child is at risk of harm must report it immediately to the DSL or member of DSL team.** In the absence of any of the above, the matter should be brought to the attention of the most senior member of staff (See staff planner for simple chart "What to do").
- 5.5. If a child is in **immediate danger or risk of harm**, a referral should be made to Children's Social Care and/or the Police immediately. Anyone can make a referral, but in situations where referrals are not made by the DSL or DSL Team, they should be informed as soon as possible afterwards that a referral has been made by someone else (see 5.10). Please see section 12 for concerns and disclosures linked to peer on peer abuse.
- 5.6 All concerns, discussions and decisions made and the reasons for those decisions should be recorded in writing using CPOMs.
- 5.7 Following receipt of any information raising concern, the DSL / DSL team will consider what action to take and seek advice from Derbyshire Starting Point, as required. All information and actions taken, including the reasons for any decisions made, will be fully documented.
- 5.8 All referrals will be made in line with Local Safeguarding partnership procedures.
- 5.9 If the child's situation does not appear to be improving the staff member with concerns should press for re-consideration by raising concerns again with the DSL; where necessary, we will consider following the local safeguarding board escalation procedures when working with external agencies to ensure better support for the child. Concerns should always lead to help for the child at some point.
- 5.10 Staff should always follow the reporting procedures outlined in this policy in the first instance. However, they may also share information directly with Derbyshire Starting Point / Sheffield safeguarding hub for Sheffield residents, or the police if: the situation is an emergency and the designated senior person, Designated Safeguarding Team and the Principal/Vice Principal are all unavailable or if: they are convinced that a direct report is the only way to ensure the student's safety

(STARTING POINT 01629 535353)

- 5.11 Any member of staff who does not feel that concerns about a child have been responded to appropriately and in accordance with the procedures as outlined in this policy should raise their concerns with the Principal or the Chair of Trustees. If any member of staff does not feel the situation has been addressed appropriately at this point, he/she should contact the Safeguarding Children's Unit directly with their concerns.
- 5.12 If staff members have concerns about another staff member then this should be referred to the Principal/Chief Executive. Where there are concerns about the Principal/Trust staff this should be referred to the Chief Executive. If concerns are about the Chief Executive this should be referred to the Chair of Trustees. Staff should also refer to our Whistleblowing Policy.

Children Missing from Education (CME)

- 5.13 Staff must be aware that children going missing, particularly repeatedly, may be a sign of a range of safeguarding possibilities including abuse (including bullying, sexual harassment, online sexual harm) and neglect, and/or criminal, sexual exploitation. It could also indicate mental health problems, risk of substance abuse, risk of travelling to conflict zones, risk of female genital mutilation (FGM) or forced marriage.
- 5.14 Registers are taken at the start of each session and also during each lesson to track/monitor attendance daily. Early intervention is necessary to try to identify underlying issues and help prevent further missing episodes.
- 5.15 When absence is unexplained, our attendance team will endeavour to contact families from the first day of absence to ascertain reasons for absence. We always ask for at least 2 emergency contacts when a child starts school.
- 5.16 We will closely monitor attendance patterns to try to pinpoint any specific issues. We work with Early Help Attendance leads to support good school attendance. Where we have serious concerns, both Children's Social Care and/or Police will be notified immediately. Within school we have a list of key vulnerable students whose attendance is always checked early each morning as a priority.
- 5.17 Positive working relationships are key to building trust between home and school to promote the importance of attendance. We also work closely with the Local Authority's Children Missing from Education Team (see Attendance Policy).

Children potentially at greater risk of harm

- 5.18 All staff should be aware that a child's experiences of adversity and trauma (**ACEs – Adverse Childhood Experiences**) can leave them vulnerable to further harm, as well as educationally disadvantaged in facing barriers to attendance, learning, behaviour and mental health. As such they may need a social worker due to safeguarding or welfare needs. Local authorities should share the fact a child has a social worker and this will be recorded on CPOMs to enable the DSL and pastoral teams to act in the best interests of the child's safety, welfare and educational outcomes.

Where a child has a social worker, this will help inform decisions about safeguarding (for example, responding to unauthorised absence or missing education where there are known safeguarding risks) and about promoting welfare (for example, considering the provision of pastoral and/or academic support, alongside action by statutory services).

Children requiring mental health support

- 5.19 Schools have an important role to play in supporting the mental health and wellbeing of students. We have a graduated response in school and should a student require support beyond tutors and heads of year, referrals can be made to our Achievement Support team for in-house support. Students can also be referred to the school nurse, the school counsellor or Early Help. For the most complex cases referrals are made to CAMHS. The DSL team and Achievement Support leads will use safeguarding meetings to monitor and review students who require support with their mental health. We also have information on our website for both students and parents (www.eckington.net).

Looked after children and previously looked after children

- 5.20 The most common reason for children becoming looked after is as a result of abuse and/or neglect. School should ensure that appropriate staff have the information they need in relation to a child's looked after legal status (whether they are looked after under voluntary arrangements with consent of parents, or on an interim or full care order) and the child's contact arrangements with birth parents or those with parental responsibility. They should also have information about the child's care arrangements and the levels of authority delegated to the carer by the authority looking after him/her along with details of the child's social worker and the name of the virtual school head in the authority that looks after the child. Our designated teacher for looked after children at Eckington School is our SEND Co-ordinator.

A **previously looked after child** potentially remains vulnerable and all staff should have the skills, knowledge and understanding to keep previously looked after children safe. When dealing with looked after children and previously looked after children, it is important that all agencies work together and prompt action is taken when necessary to safeguard these children, who are a particularly vulnerable group.

Children with special educational needs (SEN) and disabilities

- 5.21 These students can face additional safeguarding challenges and it should be noted that additional barriers can exist when recognising abuse and neglect in this group of children. These can include: -
- assumptions that indicators of possible abuse such as behaviour, mood and injury relate to the child's disability without further exploration.
 - being more prone to peer group isolation than other children.
 - the potential for children with SEN and disabilities being disproportionately impacted by behaviours such as bullying, without outwardly showing any signs; and
 - communication barriers and difficulties in overcoming these barriers.

To address these additional challenges many students have lead workers who get to know the student well and our SEND Co-ordinator is part of the DSL team.

Elective Home Education (EHE)

5.22 When a parent requests to home educate their child we will work with Derbyshire's elective home education team and implement their procedures to best support the parent making a decision in the best interests of their child and only remove from roll once the local authority have agreed to this decision.

6. RECORDS AND INFORMATION SHARING

- 6.1 If staff are concerned about the welfare or safety of any child at their Academy they will record their concern on CPOMs which records a date and time as well as the

author (see staff planner for further details). **Any immediate concerns should be passed to the DSL / DSL team without delay.**

- 6.2 Any information recorded on paper will be kept in a separate named file, in a secure cabinet and not with the child's academic file. These files will be the responsibility of the DSL. Child protection information will only be shared within Academy on the basis of 'need to know in the child's interests' and on the understanding that it remains strictly confidential. Most of our records are kept electronically via a secure service, CPOMS, which is security protected.
- 6.3 When a student leaves the Academy, the DSL will make contact with the DSL at the new Academy and will ensure that the child protection file is forwarded to the receiving Academy in an appropriately agreed manner. We will retain evidence to demonstrate how the file has been transferred; this may be in the form of a written confirmation of receipt from the receiving Academy and/or evidence of recorded delivery.
- 6.4 We are part of the **Operation Encompass** scheme. This is a unique early intervention safeguarding partnership enabling support for children and young people who may have experienced or are affected by domestic abuse. Operation Encompass will ensure that incidents of Domestic Abuse where police have attended are shared with schools, not just those where an offence can be identified. The purpose of the information sharing is to ensure schools have more information to support safeguarding of children. By knowing that the child has had this experience, the school is in a better position to understand and be supportive of the child's needs and possible behaviours.
- 6.5 **Information sharing is vital in identifying and tackling all forms of abuse and neglect, and in promoting children's welfare, including their educational outcomes. Schools and colleges have clear powers to share, hold and use information for these purposes. (KCSE 2021 p105)**
- 6.6 The Data Protection Act 2018 and GDPR do not prevent, or limit, the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to promote the welfare and protect the safety of children. (See KCSE 2021 p109)

7. WORKING WITH PARENTS & CARERS

- 7.1 LEAP Multi-Academy Trust is committed to working in partnership with parents/carers to safeguard and promote the welfare of children and to support them to understand our statutory responsibilities in this area.
- 7.2 When new students join our Academies, parents/carers will be informed that we have a safeguarding policy. A copy will be provided to parents on request and is available on each Academy website. Parents/carers will be informed of our legal duty to assist our colleagues in other agencies with child protection enquiries and what happens should we have cause to make a referral to the relevant Multi-agency safeguarding hub.
- 7.3 We are committed to working with parents positively, openly and honestly. We ensure that all parents are treated with respect, dignity and courtesy. We respect parents'/carers' rights to privacy and confidentiality and will not share sensitive information unless we have permission or it is necessary to do so in order to safeguard a child from harm.

- 7.4 We will seek to share with parents/carers any concerns we may have about their child *unless* to do so may place a child at increased risk of harm. A lack of parental engagement or agreement regarding the concerns the Academy has about a child will not prevent the DSL/DSL team making a referral to the Multi-agency safeguarding hub in those circumstances where it is appropriate to do so.
- 7.5 In order to keep children safe and provide appropriate care for them, the Academy requires parents/carers to provide accurate and up to date information regarding: -
- Full names and contact details of all adults with whom the child normally lives
 - Full names and contact details of all persons with parental responsibility (if different from above)
 - Emergency contact details (if different from above); we require at least two emergency contacts
 - Full details of any other adult authorised by the parent to collect the child from Academy (if different from the above).
- 7.6 The Academy will retain this information on the student file. The Academy will only share information about students with adults who have parental responsibility for a student or where a parent/carer has given permission and the Academy has been supplied with the adult's full details in writing (see point 6.4 and 7.4 for further details).

8. CHILD PROTECTION CONFERENCES AND OTHER MEETINGS

- 8.1 Following a Strategy Meeting, Social Care may convene a Child Protection conference and undertake a child protection enquiry under Section 47 of the Children Act if the child is judged to be at risk of significant harm.
- 8.2 A review conference will take place once a child has been made the subject of a Child Protection Plan in order to monitor the safety of the child and the required reduction in risk.
- 8.3 Staff members may be asked to attend a child protection conference or core group meetings on behalf of the Academy in respect of individual children. Usually the person representing the Academy at these meetings will be in the DSL team and/or pastoral team. In any event, the person attending will need to have as much relevant up to date information about the child as possible; any member of staff may be required to contribute to this process.
- 8.4 All reports for child protection conferences will be prepared in advance using the guidance and the template provided using the Signs of Safety format. The information contained in the report will be shared with parents/carers before the conference as appropriate and will include information relating to the child's physical, emotional and intellectual development and the child's presentation at Academy.
- 8.5 Clearly child protection conferences can be upsetting for parents/carers. We recognise that we are likely to have more contact with parents/carers than other professionals involved. We will work in an open and honest way with any parent/carer whose child has been referred to Children's Services or whose child is subject to a child protection plan. Our responsibility is to promote the protection and welfare of all children and our aim is to achieve this in partnership with our parents/carers.

- 8.6 In addition to Child Protection Conferences, staff may be asked to participate in Child in Need meetings (section 17, Children Act) and contribute to such assessments.
- 8.7 There will also be a number of other meetings, such as team around the family (TAF) meetings which may involve a range of agencies, such as Early Help, CAMHS, school nursing etc., which staff are expected to contribute to best support a student's best interests.

9. SAFER RECRUITMENT – see the LEAP Recruitment Policy for further details

- 9.1 We will ensure that at least one member of any interviewing panel has completed appropriate safer recruitment training. At all times the Principal/Chief Executive and Board of Trustees will ensure that safer recruitment practices are followed in accordance with the requirements of “*Keeping Children Safe in Education*, DfE, (2021)”.
- 9.2 Our post adverts/information packs state our commitment to safeguarding and all applications are via our standard application form that requires: employment history including reasons for leaving a post with dates, states that we will only accept references completed on our reference request forms and that no open references/testimonials or family references will be accepted and requires the candidate to declare convictions, and confirm the information they have given is correct and that they are not barred from working with children.

Shortlisted candidates will be asked to complete a self-declaration of their criminal record or information that would make them unsuitable to work with children. This self -declaration is subject to Ministry of Justice guidance. This process allows candidates to share relevant information and allow this to be discussed and considered at interview before the DBS certificate is received.

- 9.3 Within LEAP MAT Academies as part of the interview process, **candidates will have** a separate safeguarding interview led by someone who has been safer recruitment trained; this feedback informs the main interview and the final decision making.

We will always obtain references from the candidate's current employer. In addition, we will check references for candidates and **verify those for the successful candidate.** (KCSE p204)

- 9.4 Within LEAP MAT we will use the recruitment and selection process to deter and reject unsuitable candidates. We require evidence of original academic certificates and best practice for checking ID not only involves photo ID but also a birth certificate to check the name of the candidate against other forms of ID provided. We do not accept testimonials and we insist on taking up references prior to appointment. We will question the contents of application forms if we are unclear about them; we will undertake Disclosure and Barring Service checks and use any other means of ensuring we are recruiting and selecting the most suitable people to work with our children. We will also verify a candidate's mental and physical fitness to carry out their work responsibilities.

All offers of appointment are conditional on the successful completion of the mandatory pre-employment checks.

- 9.5 Each Academy will keep its own Single Central Record. We maintain a Single Central Register of all safer recruitment checks carried out in line with statutory

requirements. The Single Central Record will contain information on all staff members on the following: -

- An identity check
- A barred list check
- An enhanced DBS check/certificate
- A prohibition from teaching check
- A section 128 check [for management positions including Trustees, Governors, Senior Leadership Team (SLT) and middle leaders e.g. subject and pastoral leaders]
- A check of professional qualifications
- A check to establish the person's right to work in the UK
- Further checks on people who have lived or worked outside the UK
- Any other relevant information we feel should be included on the SCR such as volunteers, childcare disqualification, safeguarding and safer recruitment training records etc.

9.6 This record is monitored and checked every term by the Principal/Governor responsible for safeguarding and the DSL and signed off if accurate. Any issues that have been identified will be handled as a matter of urgency.

9.7 All staff are reminded that their relationships and associations in school and at home (including online) may have an implication for safeguarding students. **All staff have a duty to inform the Academy if there is a change in circumstance which may lead to possible disqualification from working with children.**

Supply Staff

9.8 If using supply agencies, we will always obtain written confirmation that the agency has carried out the relevant checks and obtained the appropriate DBS certificate. **On the single Central Record, we will note the date written confirmation is received and whether enhanced DBS check has been provided.**

School should ensure allegations about supply staff are dealt with properly and that we work with the agency to follow our safeguarding procedures; we will discuss with the agency whether it is appropriate to suspend the supply teacher or redeploy to another part of the school whilst we carry out an investigation; the agency should be fully involved and cooperate in enquiries from the LADO, police and /or social services. (KCSE 2021, 268-271)

9.9 Keeping Children Safe in Education (2021): part three – safe recruitment is the key basis for all our employment procedures and checks.

9.10 Where we use **Alternative Provision**, we will obtain written confirmation that the provider has completed the appropriate safeguarding checks on all staff working at the establishment. We will complete health and safety checks on these providers. We will ensure that staff at the provision have suitable information about our student (s) including any additional risk of harm that they may be vulnerable to. We will have regular contact with the provider to check attendance and progress of students.

9.11 If students participate in **work experience**, the Academy will ensure that the placement provider has policies and procedures in place to protect children from harm by using a recognised provider.

9.12 Barred list checks by the DBS might be required on some people who supervise a child under 16. The Academy will consider the circumstances of the placement, particularly whether the person providing the supervision/training is: -

- Unsupervised themselves and
 - Providing the supervision/training frequently (more than 3 days in 30-day period/overnight)
 - and if this is the case, then it is likely that this is regulated activity, so the person providing the supervision/training must not be a barred person.
- 9.13 The Academy is NOT able to request an enhanced DBS with barred list check for staff supervising students aged 16 or 17 on work experience.
- 9.14 If the work experience takes place in a setting which allows for contact with children and the student on work experience is 16 years old or more, the provider should consider whether a DBS enhanced check should be requested for that student.

Children Staying with Host Families (eg, foreign exchange visit/sports tour)
UK Host Families

- 9.15 The adults will be in regulated activity and the Academy would be the regulated activity provider. As such, we commit a criminal offence, if we know, or have reason to believe, an individual is barred by the DBS from engaging in regulated activity, but we allow that individual to carry out any form of regulated activity.
- 9.16 The Academy will obtain a DBS enhanced certificate with barred list information to help assess the appropriateness of whether the adult would be a suitable host for a child.

Host Families Abroad

- 9.17 The Academy will liaise with partner schools abroad, to establish a shared understanding of, and agreement to the arrangements for the visit. Staff will use their professional judgement to satisfy themselves that the arrangements are appropriate and sufficient to safeguard the student. Parents will be made aware of agreed arrangements and students will be given staff contact details should and there be an emergency/or they have any worries during the visit.

Private Fostering

- 9.18 Where the Academy becomes aware of a possible private fostering arrangement (child under 16, [under 18 if disabled] is provided with care and accommodation by a person who is not a parent, person with parental responsibility, or a relative in their own home for more than 28 days), we will notify Children’s Social Care.

10. SAFER WORKING PRACTICE

- 10.1 All adults who come into contact with our students have a duty of care to safeguard and promote their welfare. There is a legal duty placed upon us to ensure that all adults who work with or on behalf of our students are competent, confident and safe to do so.
- 10.2 Guidance about acceptable conduct and safe practice will be given to all staff and volunteers during induction. These are sensible steps that every adult should take in their daily professional conduct with children. There are circumstances, however, when it is appropriate for staff in our school to use ‘reasonable force’ to safeguard children and young people. **(See Use of reasonable force policy)**
- 10.3 ‘Reasonable Force’ covers the broad range of actions used by our staff that involves a degree of physical contact to control or restrain children. This can range from guiding a child to safety by the arm, to more extreme circumstances such as breaking up a fight or where a young person needs to be restrained to prevent violence or injury. In addition, some staff in our Academy will be trained in Team

Teach methods and a list of those who have been trained will be kept by the Principal.

- 10.4 Visitors, volunteers or parent helpers must sign in at reception and receive a visitors' badge. This must be worn and be visible at all times. Where visitors, volunteers etc. are working with children alone (ie, in regulated activity) they must have a valid DBS (enhanced DBS with barred list check) and, wherever possible, be visible to other members of staff. They will be expected to inform another member of staff of their whereabouts in Academy, who they are with and for how long. Doors, ideally, should have a clear glass panel in them and be left open. Visitors without a valid DBS must be accompanied at all times within the Academy.
- 10.5 Guidance about acceptable conduct and safe practice will be given to all staff and volunteers during induction. These are sensible steps that every adult should take in their daily professional conduct with children. This advice can be found in the LEAP Staff Safeguarding Code of Conduct.
- 10.6 'Safer working practices for adults who work with children and young people' (Safer Recruitment Consortium, May 2019, and Addendum April 2020). All staff and volunteers are expected to carry out their work in accordance with this guidance and will be made aware that failure to do so could lead to disciplinary action (See LEAP Staff Safeguarding Code of Conduct).
- 10.7 **All volunteers must be risk assessed** prior to starting to determine whether an enhanced DBS is needed for a volunteer NOT engaging in regulated activity (KCSE 2021, p290-294). Details of risk assessment will be recorded (see Volunteers Policy including request form and risk assessment as outlined in the LEAP Recruitment Procedures document).
- 10.8 **Visitors** who are in school in their **professional capacity**, will need their professional ID and we will need to be assured that they have the correct DBS checks (e.g. employer confirms this or self-employed worker shows their DBS)
- 10.9 **Contractors** in regulated activity will all have enhanced DBS (with barred list check) whilst other contractors who are not supervising students, but have opportunity for regular contact with students will have an enhanced DBS (not including barred list information). All other contractors are supervised at all times. 'Where we use contractors to provide services, we will set out our safeguarding requirements in the contract between the organisation and school (KCSE p272).
- 10.10 **Use of school site for non-school activities**
Where the school hires or rents out school premises e.g. sports associations, the governing body /business manager must make sure that safeguarding requirements are part of the contract and should ensure their policy and procedures to be submitted for review of the DSL and governing body before the contract is finalised; failure to comply would lead to a termination of the agreement (KCSE p155-16). It is the group/organisation's responsibility to safeguard users of their service.

11. MANAGING ALLEGATIONS AGAINST STAFF & VOLUNTEERS

- 11.1 Our aim is to provide a safe and supportive environment which secures the well-being and very best outcomes for the students at our Academy. We do recognise that sometimes the behaviour of adults may lead to an allegation of abuse being made.

We recognise that there are two levels of harm:

- Allegations that may meet the harms threshold.
- Allegation/concerns that do not meet the harms threshold – referred to for the purposes of this policy as 'low level concerns'.

11.2 Allegations sometimes arise from a differing understanding of the same event, but when they occur they are distressing and difficult for all concerned. We also recognise that many allegations are genuine and there are some adults who deliberately seek to harm or abuse children. We aim to deal with allegations quickly and in a fair and consistent way that effectively protects the student and at same time supports the member of staff/adult who is subject to allegation, applying common sense to our actions.

Allegations that may meet the harms threshold.

We will follow our LADO procedures if a member of staff, supply teacher, contractor or volunteer has:

- behaved in a way that has harmed a child or may have harmed a child.
- possibly committed a criminal offence against or related to a child.
- behaved towards a child or children in a way that indicates he or she may pose a risk of harm to children; or
- behaved or may have behaved in a way that indicates they may not be suitable to work with children eg behaviour out of work could be a transferrable risk when working with children

11.3 We will take all possible steps to safeguard our children and to ensure that the adults in our Academy are safe to work with children. We will always ensure that the procedures outlined in the local authority's Derbyshire's *Local Safeguarding Partnership's Child Protection Procedures*, of the statutory guidance *KCSE (2021)* section 3, particularly p338 -405, are adhered to and will seek appropriate advice from the Local Authority Designated Officer (LADO). The LADO is a statutory post appointed by the Local Authority who is responsible for co-ordinating the response to concerns that an adult who works with children may have caused or could cause harm to children. The LADO can be contacted on 01332 642376.

11.4 Who to report to: If an allegation is made or information is received about an adult who works in our setting which indicates that they may be unsuitable to work with children, the member of staff receiving the information should **inform the Principal/DSL immediately**.

Should an allegation be made against the Principal/Trust staff the **Chief Executive** should be informed; in the case of concerns about the Chief Executive then the **Chair of Trustees** should be informed. Where there are concerns about Governors, then these should be reported **to the Principal** and in the case of Trustees to the **Chair of Trustees and Chief Executive**.

In the event that the Chief Executive/Principal or Chair of Trustees is not contactable on that day, the information must be passed to and dealt with by either the member of staff acting as Principal/or the Vice Chair of Trustees.

11.5 The Chief Executive/Principal/ DSL or Chair of Trustees will **seek advice from the LADO within one working day**. No member of staff or the Board of Trustees will undertake further investigations before receiving advice from the LADO.

11.6 Any member of staff or volunteer who does not feel confident to raise their concerns with the Chief Executive/Principal/or Chair of Trustees should contact the LADO directly on 01332 642376.

- 11.7 When an allegation is made, we will consider:
- looking after the welfare of the child (referring suspected abuse to social care via Starting Point)
 - Investigating and supporting the person subject to the allegation

Before contacting the LADO, we will seek basic information, making sure not to jeopardise any future police investigation. Information may include- was the individual in school at time of allegation? Did they come in contact with the child? Any witnesses? Any CCTV footage? Personal data about the individual will also be required by the LADO e.g. address, do they have or live with any children under 18?

- 11.8 The school will work with the LADO, police and social care to support the LADO investigation process and agree what information can be shared with parents of students involved and others involved in the investigation as well as the requirement to maintain confidentiality. HR will be involved in this process and careful consideration will be given to any decision to suspend a colleague (see KCSE p361-368).

- 11.9 Allegation outcomes:
- **Substantiated:** there is sufficient evidence to prove the allegation.
 - **Malicious:** there is sufficient evidence to disprove the allegation and there has been a deliberate act to deceive or cause harm to the person subject of the allegation.
 - **False:** there is sufficient evidence to disprove the allegation.
 - **Unsubstantiated:** there is insufficient evidence to either prove or disprove the allegation. The term, therefore, does not imply guilt or innocence; or,
 - **Unfounded:** to reflect cases where there is no evidence or proper basis which supports the allegation being made.

The Academy has a legal duty to refer to the Disclosure and Barring Service anyone who has harmed, or poses a risk of harm, to a child, or if there is reason to believe the member of staff has committed one of a number of listed offences, and who has been removed from working (paid or unpaid) in regulated activity, or would have been removed had they not left or they are suspended. The DBS will consider whether to bar the person. If these circumstances arise in relation to a member of staff at our Academy, a referral will be made as soon as possible after the resignation or removal of the individual in accordance with advice from the LADO and/or HR. If this should happen we will ensure that at the conclusion of a case we will review our procedures or practice to help prevent similar events happening in the future.

See KCSE p381-405 for further details

- 11.9 A summary of managing allegations about staff is included in the staff planner for easy reference.

11.10 Allegations/**concerns that do not meet the harm threshold**

As part of our holistic approach to safeguarding we promote an open culture in which all concerns about adults are dealt with promptly and appropriately, this includes concerns from students, parents, staff or as a result of information received via vetting checks. We would also encourage staff to self-refer when they have found themselves in a situation which could be misinterpreted, might appear compromising or they have behaved in a way that falls below professional standards.

Where such a concern does not meet the harm threshold described above (eg over friendly with child(ren), inappropriate language used, or where behaviour falls below professional standards outlined in the Staff Safeguarding Code of Conduct, Teacher Standards), a concern should still be brought to the attention of the DSL.

We recognise that such behaviour exists on a broad spectrum ranging from a thoughtless comment to behaviour that may look to be inappropriate, but might not be in specific circumstances, through to that which is ultimately intended to enable abuse.

Procedure for sharing low- level concerns:

Where staff, students or parents have a concern about staff conduct, they should always report this to the Principal (KCSE p416)

Concerns will be dealt with in a sensitive and timely manner, supporting the individual to correct behaviour at an early stage.

The Principal will collect as much evidence as possible by speaking to the person who has raised the concern, to the individual involved and any witnesses.

This information will help to categorise the behaviour and determine further action.

The Principal will record all low level concerns detailing the details of the concern, the context and action taken. The name of the person sharing the concern should be noted, but if the wish to remain anonymous then that will be respected as far as is reasonably possible. These records are confidential and will be kept at least until the colleague leaves employment at the LEAP Trust. We would normally write to the colleague involved, summarising our actions.

Where concerns involve a third-party colleague e.g. supply, then the same procedures will be undertaken and their employer also notified.

Low level concerns will not be shared in references unless they relate to issues which would normally be included in a reference e.g. misconduct, poor performance. Where a concern met LADO thresholds and was substantiated, it will be referred to in a reference. (KCSE 422)

Patterns of behaviour will be reviewed to decide future actions including possible LADO referral.

We will use incidents to review of safeguarding practice and make improvements as appropriate.

12. CHILD ON CHILD SEXUAL VIOLENCE AND SEXUAL HARRASSMENT

- 12.1 As noted in section 1.7 of this policy, all staff, volunteers and visitors as well as governors and trustees must work together consistently to embed an ethos of recognising and addressing all forms of sexual harassment and implementing sanctions where appropriate. **We have a statutory duty to respond to all reports and concerns of child on child sexual violence and harassment, including those that have happened outside school and online (KCSE p427).** Peer on peer sexual violence and harassment exists on a continuum (see point 12.3 below) and may overlap; they can happen face to face and online and are **never acceptable; as such we have a zero-tolerance approach to sexual violence and sexual harassment** (KCSE p449).

Addressing inappropriate behaviour, no matter how innocuous, can be an important intervention that helps prevent problematic, abusive or violent behaviour in the future. **We recognise that if incidents are not addressed then this can lead to a culture of unacceptable behaviour, an unsafe environment where such abuse is normalised, accepted and children fail to report it.**

12.2 Staff will reassure victims that they are being taken seriously, they have done the right thing to report an incident and that we will work to keep them safe. Staff are also aware that girls are likely to be victims of sexual violence and harassment whilst boys are more likely to be perpetrators.

12.3 **What do we mean by sexual violence and harassment?**

Sexual violence refers to criminal acts:

- Rape
- Assault by penetration
- Sexual assault (intentional sexual touching where the person does not consent)

It should be noted that consent is key and that a child under 13 can never consent to any sexual activity; the age of consent is 16 years old. Sexual intercourse without consent is rape.

Sexual harassment refers to unwanted conduct of a sexual nature.

- sexual comments e.g.: telling sexual stories, making lewd comments, sexual remarks about clothes and appearance and calling someone sexualized names
- sexual “jokes” or taunting
- physical behaviour – e.g. deliberately brushing against someone, interfering with someone’s clothes (check the cross into sexual violence - it is important to talk to the victim) and displaying pictures, photos or drawings of a sexual nature

Online sexual harassment. This may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence. It may include:

- non-consensual sharing of sexual images and videos
- sexualised online bullying
- unwanted sexual comments and messages, including, on social media
- sexual exploitation; coercion and threats

Harmful sexual behaviour is an umbrella term recognising that children’s sexual behaviour exists on a wide continuum ranging from normal through to violent as shown in the diagram below:

Normal	Inappropriate	Problematic	Abusive	Violent
Developmentally expected	Single instances of inappropriate behaviour	Problematic and concerning behaviours	Victimising intent or outcome	Physically violent sexual abuse
Socially acceptable	Socially acceptable behaviour within peer group	Developmentally unusual and socially unexpected	Includes misuse of power	Highly intrusive
Consensual, mutual, reciprocal	Context for behaviour may be inappropriate	No overt elements of victimisation	Coercion and force to ensure victim compliance	Instrumental violence which is physiologically and/or sexually arousing to the perpetrator
Shared decision making	Generally consensual and reciprocal	Consent issues may be unclear	Intrusive	Sadism
		May lack reciprocity or equal power	Informed consent lacking, or not able to be freely by victim	
		May include levels of compulsivity	May include elements of expressive violence	

12.3 Preventative measures:

Education is vital part of our work to help students to understand that sexual harassment and online abuse will not be tolerated and that our school community in particular needs to be a safe place for all. Our Character curriculum is a key driver for this education process, particularly the Relationships, sex and health education (RSHE) element of the curriculum. This will be reinforced through our morning guidance work, including assemblies, and Flexible Days where the concept of respect is a key theme.

We will continue to garner student views via student voice activities – including on line surveys and discussion groups to help ensure that our curriculum meets need and reduces the gap in perception between students and staff. As part of student voice work we will continue to establish hot spots within our setting to help us better address issues and concerns. Hot spots locally will be discussed with Early Help locality leads and community police.

12.4 Supporting students to report concerns:

We will continue to work with student groups to develop ways students can report issues.

At present, we encourage students to speak to the DSL team or ANY member of staff they trust and feel able to talk to.

Our “What happens next when you report a concern?” poster summaries what students can expect when they express a concern about harassment of online abuse:

- staff will listen, not judge
- staff will consider what they have been told and how the school can help keep you safe
- they will discuss this with the safeguarding team
- staff will talk to you about your views and balance this with keeping you and others safe
- explain the range of actions possible: internal, Early Help, Social Care and /or Police involvement

- Use the Behaviour policy to implement sanctions where appropriate

12.5 Responding to reports/concerns

We know that some children will find it difficult to report incidents and may ask a friend to do so or staff may overhear a conversation or have concerns about a child's change in behaviour/presentation.

- Reassure the victim, that they are being taken seriously as noted above in 12.2; this helps instil confidence in the victim and create a whole school supportive culture.
- Staff should follow our general safeguarding guidelines for handling a disclosure: -
 - Reassure, notably
 - Not promising confidentiality
 - Listening carefully, not asking leading questions
 - Recording the facts as presented
 - Notify DSL Team immediately
 - Where there is an allegation about online sexual abuse, staff follow the searching and screening policy and do NOT view the image
 - Have 2 members of staff present where possible
- DSL team will then review this initial disclosure and reassure the victim that they will be supported and kept safe. Immediate consideration will be given as to how best to support and protect the victim and the alleged perpetrator (and others involved) as part of our **risk assessment process** as well as balance the victim's wishes against our responsibility to protect them and other children.
- Reports of sexual violence and sexual harassment are likely to be complex and require difficult professional decisions to be made, often quickly and under pressure. Decisions need to be made on a case by case basis with the DSL (DSL Team) taking a leading role, supported by partnership agencies such as Children's Social Care and Police.

12.6 In the case of sexual violence, DSL/DSL Team will make an **immediate risk and needs assessment** (sexual harassment the need for a risk assessment considered on case by case basis) to consider: -

- Victim, especially their protection, and support alleged perpetrator
- All the other students (and if appropriate adults/staff)

These assessments will be recorded and kept under review.

12.7 The DSL/DSL Team will work closely with Children's Social Care and other specialist Services.

Action Following a Report of Sexual Violence/Sexual Harassment

12.8 Sexual violence and abuse can happen anywhere and all staff need to maintain the attitude that "it could happen here". Staff will always consider:

- Wishes of victim to help give them as much control as is reasonably possible balanced with or duty to protect other children
- Nature of alleged incident and whether crime may have been committed
- Age of students and developmental stage of those involved
- The power balance between the students
- If the alleged incident is one off or part of a pattern of abuse
- Sexual harassment and violence within intimate personal relationships between peers
- Ongoing risks to victim, other students or adults
- Other contextual safeguarding concerns beyond school e.g. links to CCE , CSE

Sharing a Classroom

- 12.9 Any report of sexual violence, is likely to be traumatic for the victim. Whilst the school establishes the facts of the case and starts the process of liaising with Children's Social Care and Police, the alleged perpetrator should be removed from any classes they share with the victim.
- 12.10 We will consider how best to keep victim and alleged perpetrator a reasonable distance apart on the Academy premises and transport to/from school each day. These actions are in the interests of **BOTH** children and should not be seen as judgmental.
- 12.11 In other cases of sexual harassment, the wishes of the victim, the nature of the allegations and the protection of children in school will be important when considering any immediate actions.

Managing Reports

- 12.12 Reports will be managed on a case by case basis and generally with advice from appropriate agencies.
- 12.13 There are 4 key possible scenarios, however each one is **under-pinned by the principle that there is a zero-tolerance approach to sexual harassment and sexual violence and it will never be tolerated.** In all cases written records will be kept.
- a) Manage internally
It is considered for a possible one-off incident to handle the incident internally in line with Behaviour and Anti-bullying policies to reinforce sexual harassment/violence is never acceptable.
- b) Early Help
Following from the above, there is no requirement for statutory interventions again, however, the Academy believes support from Early Help would be beneficial to prevent any escalation of such behaviours
- c) Referral to Children's Social Care
Where a child is harmed, is at risk of harm or is in immediate danger, we will make a referral to MASH. We will work closely with Social Care to protect the student(s) involved and not jeopardise a statutory investigation.
- d) Referral to Police
Referral to Police should be done in parallel with a referral to Children's Social Care as outlined at (c) above. In the case of sexual violence, the starting point is the police. We will liaise with the police as to what information can be shared, particularly what can be shared with the alleged perpetrator and their parents/carers.
- 12.14 Risk assessments will be immediately drawn up and will remain in place and under review throughout a criminal investigation/progression through criminal justice system to protect the victim, alleged perpetrator and other students. The Academy will work with the Police to ensure any actions the Academy takes do not jeopardise the Police investigation.
- 12.15 If a child is convicted or receives a caution for a sexual offence, the Academy will update risk assessments to protect all students and if it has not already done so, consider suitable action in light of behaviour policy, including permanent exclusion.

- 12.16 If the perpetrator remains in school, clear expectations of behaviour will be outlined along with any restrictions the Academy thinks are reasonable and proportionate with regard to the perpetrator's timetable.
- 12.17 The Academy will work to ensure that both the victim and perpetrator are protected, particularly from bullying.
- 12.18 Where there is a 'no further action' or not guilty verdict, the Academy will continue to support the victim and alleged perpetrator.
- 12.19 If a report is determined to be unsubstantiated, unfounded, false or malicious, we will consider whether the child and/or the person who has made the allegation is in need of help or may have been abused by someone else and this is a cry for help. In such circumstances, a referral via MASH may be appropriate.

If a report is shown to be deliberately invented or malicious, we will consider whether any disciplinary action is appropriate against the individual who has made it.

Supporting the Victim

- 12.20 Throughout this whole process, the needs and wishes of the victim are paramount (along with protecting them) in any response. Our **overall priority is to make the victim's daily experience as normal as possible**, so that the Academy is a safe space for them. However, it is through close working with the victim that a suitable support mechanism is put in place and this is reviewed regularly as we understand that victims may not talk about the whole picture immediately. Sexual assault can result in a range of health needs and we will signpost support as necessary. (See KCSE pages 115-117 for links to national support services: Keeping Children Safe in Education).
- 12.21 Where there is a **criminal investigation** into a rape, assault by penetration or sexual assault, the alleged perpetrator should be removed from any classes they share with the victim. The Academy also needs to consider how best to keep the victim and alleged perpetrator a reasonable distance apart on the Academy premises and transport to/from school. This is in the best interests of both students and should not be perceived to be a judgment on the guilt of the alleged perpetrator. This decision will require close liaison with police.

Supporting the Alleged Perpetrator

- 12.22 This is a difficult balancing act to safeguard the victim (and wider student body) and provide the alleged perpetrator with an education, safeguarding support as appropriate and implement any disciplinary sanctions.

At the end of the criminal process, the risk assessment should be updated in light of outcomes. Where there has been a conviction or caution for rape or assault by penetration, will consider any suitable action in line with our behaviour policy, if we have not already done so. In all but the most exceptional of circumstances, the rape or assault is likely to constitute a serious breach of discipline and lead to the view that allowing the perpetrator(s) to remain in the same school would seriously harm the education or welfare of the victim (and potentially other pupils or students).

Where a criminal investigation into sexual assault leads to a conviction or caution, the school should, if it has not already, consider any suitable sanctions in light of our behaviour policy, including consideration of permanent exclusion. Where the perpetrator(s) is going to remain at the school, the principle would be to continue keeping the victim and perpetrator(s) in separate classes and continue to consider the most appropriate way to manage potential contact on school premises and

transport. The nature of the conviction or caution and wishes of the victim will be especially important in determining how to proceed in such cases.

In cases where the report of sexual violence to the police did not progress or a not guilty verdict is reached, does not mean that the victim lied.

12.23 Unsubstantiated, unfounded, false or malicious reports

All concerns, discussions and decisions should be recorded to enable them to be reviewed so that potential patterns of concerning, problematic or inappropriate behaviour can be identified and addressed. This includes considering if the person who made the allegation is in need of support

12.24 In our actions we will consider the age and developmental stage of the alleged perpetrator, along with the proportionality of our response. Advice will be taken as appropriate from Children's Social Care, Police and other specialist services.

ONLINE SEXUAL HARASSMENT: CREATING OR SHARING NUDE AND SEMI-NUDE IMAGES

12.25 Creating or sharing nude and semi-nude pictures, videos or live streams by young people of under 18s (including those created and shared with consent) is illegal which makes responding to incidents involving children complex. (Sharing nudes and semi-nudes guidance for education settings). Our response to an incident will differ depending on the motivations behind the incident and the appropriateness of the child's behaviour.

12.26 Incidents can be categorised as:

a) aggravated: incidents involve additional/abusive elements. It may involve an adult, there may be intent to harm or involve reckless behaviour.

b) experimental: incidents of creating and sending with no adult involvement, no apparent intent to harm or reckless misuse.

<p>Aggravated incidents involve criminal or abusive elements beyond the creation, sending or possession of youth-produced sexual images</p>	<p>Adult offenders attempt to develop relationships by grooming teenagers, in criminal sex offenses even without the added element of youth-produced images. Victims may be family friends, relatives, community members or contacted via the Internet. The youth-produced sexual images may be solicited by adult offenders.</p>
	<p>Youth Only: Intent to Harm cases that:</p> <ul style="list-style-type: none"> • arise from interpersonal conflict such as break-ups and fights among friends • involve criminal or abusive conduct such as blackmail, threats or deception • involve sexual abuse or exploitation by young people.
	<p>Youth Only: Reckless Misuse</p> <p>No intent to harm but images are taken or sent without the knowing or willing participation of the young person who is pictured. In these cases, pictures are taken or sent thoughtlessly or recklessly and a victim may have been harmed as a result.</p>
<p>Experimental incidents involve the creation and sending of youth-produced sexual images, with no adult involvement, no apparent intent to harm or reckless misuse.</p>	<p>Romantic episodes in which young people in ongoing relationships make images for themselves or each other, and images were not intended to be distributed beyond the pair.</p>
	<p>Sexual Attention Seeking in which images are made and sent between or among young people who were not known to be romantic partners, or where one young person takes pictures and sends them to many others or posts them online.</p>
	<p>Other. Cases that do not appear to have aggravating elements, like adult involvement, malicious motives or reckless misuse, but also do not fit into the Romantic or Attention Seeking sub-types. These involve either young people who take pictures of themselves for themselves (no evidence of any sending or sharing or intent to do so) or pre-adolescent children (age 9 or younger) who did not appear to have sexual motives.</p>

12.27 When matters come to light, DSL team staff will review the situation in light of the above as well as considering if the child is at immediate risk and if so then a referral to Starting Point and /or police will be needed.

When assessing the risk, some key questions to consider are: why was the image shared? Was it consensual? Coerced? Has the image/video been shared beyond its intended recipient? Was it shared with consent? How far has it been shared? Have steps been taken to remove it? How old are the children involved? Are there additional vulnerabilities? Are there additional concerns if parents/carers are informed?

12.28 An immediate referral to Starting Point and /or police should be made if:

- The incident involves an adult
- There is reason to believe that a child or young person has been coerced, blackmailed or groomed, or there are concerns about their capacity to consent (e.g. SEN)
- What you know about the images or videos suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
- The images involves sexual acts and any pupil in the images or videos is under 13
- You have reason to believe a child or young person is at immediate risk of harm owing to the sharing of nudes and semi-nudes, for example, they are presenting as suicidal or self-harming

12.29 Ordinarily, the image/video **must not be viewed** and staff should rely on a student's description of the image/video. Only the DSL should view the image if that is the only way to decide whether to involve other agencies because we cannot establish the facts from the student or it is necessary to report it to a website to have it removed. If this is the case, then a written record should be kept stating why the decision was made to view, who was in the room as the DSL viewed it (this second

person does not view the image). If possible, the person viewing should be of the same gender as young person in the image/video.

- 12.30 **Images will never be copied/stored as this is illegal.** If evidence needed, then the device should be turned off, confiscated and stored securely until the police collect it.
- 12.31 It is important to talk to the student involved and reassure them. Staff will need to support their parents/carers to understand the wider issues and motivations around this incident. It is important to remain solution-focused and avoid any victim-blaming questions. Use questions such as 'describe what happened' or 'explain to me who was involved' help the student to understand what has happened by discussing the wider pressures that they may face and the motivations of the person that sent on the image(s). Staff should discuss issues of consent and trust within healthy relationships as well as explain the law on the sharing of nudes and semi-nudes. It is important to highlight that the law is in place to protect children. Staff should signpost to the IWF and Childline's Report Remove tool at www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobilesafety/sexting/report-nude-image-online/
This must be done as soon as possible in order to minimise the number of people that have seen the picture.
- 12.32 We do not want to criminalise students, particularly where the situation has been assessed as "experimental". In these cases, the school will often deal with the matter internally working with the students and their parents/carers and may involve our local school police officer as part of an educational conversation/episode. However, where the incident is deemed as "aggravated" then social care, via MASH and/or the police will be involved.
- 12.33 Students who have received the images or re-shared them will be usually asked to delete them (unless the device is confiscated for the police to review). They will be asked for details of who they have shared the images with as well as trying to understand their motivations for sharing and what they could have done differently. They should also be advised on the law. Again, parents/carers and the school police officer maybe involved in these educational conversations.

13. E-SAFEGUARDING: USING TECHNOLOGY

- 13.1 The internet and other technologies play a key role in 21st Century teaching and learning and the aim of this policy is to maximise safeguarding whilst promoting the effective use of such technologies to enhance teaching and learning. This section of our policy is designed to:
- set out the key principles expected of all members of the school community with respect to the use of ICT
 - safeguard and protect students, staff and occasional visitors/users of the school's ICT infrastructure
 - set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use, having clear structures to deal with online abuse such as cyberbullying which are cross referenced with other Trust/school policies
 - ensure that all members of the LEAP Multi-Academy Trust (MAT) community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken
 - minimise the risk of misplaced or malicious allegations against adults who work with students.

SCOPE

- 13.2 The Education and Inspections Act 2006 empowers Principals, to such extent as is reasonable, to regulate the behaviour of students or students when they are off the school site. This is pertinent to incidents of cyber-bullying, or other actions covered by this policy which may take place outside of school sites, on internet platforms and be perpetrated on personal devices but is still linked to membership of the school/LEAP MAT. The school will deal with such incidents within this policy and parents/carers may be informed of concerns.
- 13.3 **The Education Act 2011 gives school the power to confiscate and search the contents of any mobile device if the Principal believes it contains any material that could be used to bully or harass others, or used to commit an offence. These devices can have data removed before they are returned.** (see the Trust's Searching, Screening & Confiscation Policy).
- 13.4 Staff and students are also bound by the Acceptable Use Agreement (AUP).

14. ROLES & RESPONSIBILITIES

14.1 Principal and DSL: Responsible for:

- Shaping and applying this policy (and other relevant policies) and ensuring staff and student safety within school
- Ensuring that staff receive relevant and suitable training and continued development to enable them to carry out their roles using ICT and implement procedures
- Reviewing and responding to any eSafeguarding incident escalated to senior leaders as well as reviewing reports from the IT team
- Liaising with the LEAP MAT/Academy IT Teams.

14.2 IT teams: Responsible for:

- Ensuring LEAP MAT's ICT infrastructure and devices are secure and not open to misuse or malicious attacks in line with this guidance and policy
- Liaising with the DSL and Principal and providing technical expertise and assistance where appropriate.

14.3 All staff: Responsible for:

- Implementing all eSafeguarding related policies
- Reporting any suspected misuse of ICT or breach of eSafeguarding policy to SLT
- Applying staff Acceptable Use Policy (AUP), GDPR working practices document and other related policies
- Embedding eSafeguarding into all aspects of the curriculum and other school activities wherever possible
- Ensuring students understand and adhere to the LEAP MAT Acceptable Use Policy
- Ensuring students have a good understanding of research skills, uphold copyright regulations for text, images and media from the internet, and avoid plagiarism
- Using good classroom management, and the provided software tools to monitor ICT activity in lessons, extra-curricular and other school activities
- Pre-checking any lesson resources that require internet access or services, and that the resources or subsequent searches have suitable content.

14.4 Students: Responsible for:

- Using our ICT services in accordance with this policy, and the AUP

- Understanding good research skills, and the need to avoid plagiarism and breaking copyright regulations
- Reporting any abuse, misuse or accidental access to inappropriate materials
- Following the school policy on mobile device use
- Understanding the consequences of breaching eSafeguarding policies, understanding why they are in place, and the impact of illegal activities such as hacking and cyber-bullying
- Understanding the importance of responsible use of digital technologies, and social media platforms out of school and realising that their personal responsibility

14.5 **Parents and Carers**

Parents and carers play a vital role in ensuring that their children understand the need to use the internet, gaming and mobile devices in a responsible and safe way. Whenever possible the Trust/Academy will take every opportunity to help parents and carers understand the issues regarding eSafeguarding through regular communications via normal and social media channels. Parents and carers are responsible for:

- Supporting and endorsing Trust/Academy policies and the members of staff who apply them
- Amplifying good and safe use of the internet and mobile devices at home, such as ensuring their children's internet connections are filtered and devices and consoles are correctly configured with parental controls to restrict inappropriate age-related games and content

15. **MANAGING ICT**

15.1 LEAP MAT is responsible for ensuring that access to ICT is as safe and secure as reasonable possible, and that policies and procedures approved within this policy are implemented:

- All users will have clearly defined rights to access ICT services, with student access based upon the principle of least privilege
- All users are issued with a unique, individually named, or numbered account used to access ICT and Office 365 services. LEAP MAT/its Academies have a pragmatic approach to the frequency of password changes, considering the potential impact on effective teaching and learning time
- The responsibility for user accounts lies with the individual, and users must not allow others to access services using their credentials and must immediately report any suspicion or evidence that their accounts have been compromised. The school will enforce sanctions to any student attempting to access other user accounts
- Any requests for changes to user accounts, in terms of permissions, or access to other services can be made on the respective school IT Helpdesks
- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access. All hardware and software, including anti-virus and anti-malware, will be kept updated as appropriate
- Guest accounts are available for visitors and can be made available with the agreement of the respective site IT teams. Where possible, guests must be encouraged to access presentations or other material via internet-based services, and not bring personal devices or removable storage into schools
 - Neither staff nor students should install programs or other software on ICT systems without the prior express permission of the respective site IT Team
 - **Access to ICT within LEAP MAT/ its Academies is a privilege and not a right and may be withdrawn at the discretion of SLT**
 - All access to the internet will be filtered

- For information on protection of Personal Data, held on site and accessible via ICT services, such as e-mail please consult LEAP MAT's GDPR and Data Handling policies/ GDPR working practices document.

16. PREVENTING THE SPREAD OF MALICIOUS SOFTWARE (MALWARE, VIRUSES AND CRYPTOWARE)

- 16.1 Users of the school's IT services must take all reasonable steps to prevent the transmission or receipt of malicious software, such as computer viruses or malware.
- 16.2 Users:
- Must not use any type of removable storage on LEAP MAT ICT infrastructure
 - Must ensure that effective anti-virus and anti-malware applications are operating on any personal device that they use to access LEAP MAT infrastructure, and that devices are regularly scanned and are free from infection
 - Must not open email attachments they have received from an unsolicited, untrusted or dubious source, or unexpected attachments from trusted sources; they should contact the IT Team
 - Must take care when entering their network credentials into sites that could attempt to harvest usernames and passwords. Users should familiarise themselves with the latest information on phishing and other forms of electronic scams

17. RESPONSIBLE USE

- 17.1 All staff and students are expected to be responsible users of ICT.
- 17.2 All users accessing ICT services agree to adhere to LEAP MAT's Acceptable Use Policy (AUP) that is displayed on PCs when first accessing the network. The AUP supplements this policy and makes all users aware of their expected responsibilities, and that all activities using ICT services, especially the use of the internet will be monitored. In addition, copies of the AUP can be found in both student and staff planners.

18. MISUSE

- 18.1 Illegal and inappropriate use of ICT services will not be tolerated. Students and staff may face disciplinary action if they engage in any such activities, including Cyber-bullying and bypassing internet filtering, or the use of electronic communication to radicalise others. They will also face disciplinary action if they post damaging or offensive comments, and/or abusive images towards other members of staff or students on any digital platform, via e-mail or any unspecified electronic medium. Should a complaint be made to school, the Trust will immediately suspend and remove access rights until the complaint is investigated and resolved.
- 18.2 In circumstances where it is assessed that there has been a breach of the standards of acceptable use, the school will, as a first action, act promptly to prevent continuance or repetition of the breach, for example to withdraw any unacceptable materials and then follow the Trust's usual disciplinary procedures. This action will involve liaison between the appropriate member(s) of staff, SLT and IT Support.
- 18.3 Note: The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the appropriate authorities.

19. REMOVING EVIDENCE FROM DIGITAL DEVICES

- 19.1 In accordance with the DfE Searching, Screening Guidance and our LEAP MAT policy, if a member of staff has grounds to suspect that a digital device contains inappropriate material, or material that has been used in an incident of misuse or breach of eSafeguarding Policy, they will seek consent from the student that the material is removed from the device or in some circumstances shared with school before it is removed.
- 19.2 **IMPORTANT NOTE:** If it is believed that the **image/recording is of a sexual nature**, it must NOT be shared with school – this is illegal. The student should be instructed to remove the image unless it is believed to be part of an aggravated incident and the evidence may be needed: then the device should be turned off, confiscated and stored securely until the police collect it.
- 19.3 Staff should seek the relevant responsible Pastoral Team or member of SLT to accompany the student to the IT Team and connect their device to an appropriate computer. To mitigate exposure to potential illegal or other inappropriate or private material, the student to locate the required file(s) and move them from the device to a secure location on the school's network.
- 19.4 A member of the IT Team will remain present to assist if required, and to act as witness.
- 19.5 **It is the responsibility of the Pastoral Team or member of SLT to retain an accurate record of evidence that has been taken from digital devices – this could be done on CPOMS.**

20. MANAGING DIGITAL CONTENT

Recording

- 20.1 Students and staff will **only use Trust equipment to create mixed digital media** (images, video and sound) of individuals within our school community. GDPR working practices document (section 19) also clearly states that **staff are not permitted to use personal devices to photograph or record images of students; any digital content must be recorded on the school's equipment.**

Using Images, Video and Sound

- 20.2 Parents or carers are informed that photographs and digital images of students may be used in the following situations:
- On the LEAP MAT and school website, school's learning platforms
 - On the LEAP MAT and school's social media pages
 - In the school prospectus and other printed promotional material, e.g. newspapers
 - In display material that may be used around the school
 - In display material that may be used off site
 - In any material that is submitted to an exam board for assessment
 - Through any external publication, e.g. Newsletter, School Year Book
 - Recorded or transmitted on a video, audio or via webcam e.g. in an educational conference or promotional video
- 20.3 Consent for these purposes is sought via the school admissions document and the privacy notice (see Trust GDPR Policy). Parents and carers may withdraw permission, in writing, at any time.
- 20.4 We will remind students of safe and responsible behaviours when creating, using and storing digital images, video and sound linked to both their schoolwork and their social use of technology. We will also remind students of the risks of

inappropriate use of digital images, video and sound in their online activities both at school and at home.

Storage of Images

- 20.5 Any images, videos or sound clips of students must be stored on the school network and never transferred to personally-owned equipment.
- 20.6 Students and staff are not permitted to use personal devices for storage of any images, videos or sound clips of students/staff or store sensitive information (GDPR working practices document - section 10).

Office 365 – SharePoint and Teams

- 20.7 LEAP MAT promotes the use of Microsoft's Office 365 suite to enhance teaching and learning and to enable learning anywhere via shared resources, email, Sharepoint and classroom hubs in "Team" sites.
- 20.8 It is the responsibility of any member of staff who creates a Sharepoint library, "Team" site or shared resource to ensure the correct sharing/access security is set, to monitor and moderate that resource, and to use the tools available to them to deal with inappropriate behaviour or content.

Parental/carer consent must be in place for students to be able to access Teams and Live Lessons. Consent for these purposes is sought via the school admissions document and the privacy notice (see Trust GDPR Policy). Parents and carers may withdraw permission, in writing, at any time.

To ensure safeguarding and conduct within meetings, **students will be required to wait in a lobby** until a member of staff is present. All student cameras are disabled, and the meeting and chat will be recorded and monitored.

All staff and students must adhere to the Trust's expectations as outlined in our acceptable use policies and also in the summary code of conduct in Appendix 6

- 20.9 To enhance eSafeguarding, some Office 365 services are restricted to students, including the use of Skype, Chat, Yammer and Kaiza.

Office 365 - Storage

- 20.10 Office365 provides each staff member and student with a storage mechanism called OneDrive that can be used to create, access and edit files from any internet-enabled device.
- 20.11 Use of OneDrive must be limited to documents such as Word, Excel and Powerpoint, but can store and manipulate images, videos and sound clips under the direction of teaching staff with permission from the Principal. When using Office 365, staff and students must abide by this policy and all relevant laws regarding the storage and sharing of illegal content.

21. CURRICULUM: Learning and Teaching

- 21.1 Online Safeguarding will be embedded across the school in a series of specific online safety/online safeguarding-related lessons in specific year groups as part of the ICT and Character curriculum in particular.
- 21.2 We will celebrate and promote online-safeguarding through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day, theatre in education visits (e.g. CSE/grooming), healthy relationships, fake news, extremism and anti-bullying assemblies.

- 21.3 Students will be taught about online safety and harms. This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online.
- 21.4 We will discuss relevant online safeguarding messages with students routinely wherever suitable opportunities arise during all lessons. This will include the need to protect personal information, to consider the consequences their actions may have on others, to check the accuracy and validity of information they use and to respect and acknowledge ownership of digital materials.
- 21.5 We will remind students and staff about their responsibilities through an **Acceptable Use Policy** which will be displayed when a student logs on to the school network. This will also be displayed in student and staff planners.
- 21.6 Staff will model safe and responsible behaviour in their own use of technology during lessons.
- 21.7 We will teach students how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area.
- 21.8 All staff and students will be taught about copyright in relation to online resources and will be taught to understand about ownership and the importance of respecting and acknowledging copyright and ownership of digital materials (this is particularly relevant for those completing coursework and essays where credit must be given to the sources used).
- 21.9 When using digital mixed media, staff will educate students about the risks with taking, using, sharing, publication and distribution of content – in particular they should recognise the risks attached to publishing comments, or media, especially images on the internet, e.g. on social networking sites such as Tik Tok and Snapchat.
- 21.10 Students will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the **CLICK CEOP** button which is on our school website along with other organisations as signposted from the website safeguarding page. Advice and support information is also in the student planners. Termly safeguarding newsletters also regularly features online safety advice for parents and staff. We will share how students and their families can gain advice about having content /images removed: www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobilesafety/sexting/report-nude-image-online/.

22. STAFF AWARENESS AND TRAINING

- 22.1 LEAP staff receive regular information and training on online safeguarding issues as part of ongoing safeguarding training/awareness raising. The termly safeguarding newsletter to staff and parents usually includes at least one article linked to online safety with regular features about apps, gaming and signposting to sources of advice and support. The safeguarding page of the school website also includes several sources of information and links to advice and support (e.g. Childnet, NSPCC, Think U Know) as well as the **CEOP support button on the opening page of the website**. The LEAP safeguarding staff Code of Conduct also outlines responsibilities linked to online safeguarding.

22.2 As part of the induction process all new staff receive information and guidance on online safeguarding and the Trust's Acceptable Use Policies (AUPs). Acceptable use policies are in both student and staff planners. Annually, staff sign to state that they have received and accept our AUP, GDPR working practices document and Code of Conduct. Online safeguarding is also one element within the annual e-learning safeguarding training all staff complete.

22.3 All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of online safeguarding and know what to do in the event of misuse of technology by any member of the school community.

23. EMERGING TECHNOLOGIES

23.1 LEAP MAT is keen to harness any emerging technologies that could benefit work practices and teaching and learning. Any new technology will be assessed and evaluated for benefit and security risks before its use is allowed in school.

- The school will periodically review which technologies are available within the School for any security vulnerabilities that may have been discovered since deployment
- Prior to deploying any new technologies within the school, staff and students will have appropriate awareness training regarding safe usage and any associated risks
- The school will monitor ICT equipment usage to establish if the e-Safeguarding policy is adequate and that the implementation of the e-Safeguarding policy is appropriate
- Methods to identify, assess and minimise risks will be reviewed regularly

24. INTERNET ACCESS

24.1 LEAP MAT's internet web filtering policy has been developed to help our schools maximise the safety of our students as they use the internet, whilst at the same time retaining the flexibility needed for effective teaching and learning.

24.2 LEAP MAT appreciates that supervision and education in the use of the internet is paramount, and undertaken as part of our Safeguarding training, as the filtering of internet connections alone cannot guarantee the absolute safety of students and staff.

Primary Filtering

24.3 Eckington School internet connections are filtered using the FortiGate 100F next-generation firewall. FortiGate uses the latest technology to block access to malicious, hacked or inappropriate websites.

Secondary Filtering

24.4 Eckington School computers utilise a remote and classroom management tool called Impero, that monitors content accessed by staff and students and uses a keyword detection solution to monitor, capture, block and report topics such as self-harm, bullying, extremism and more.

Bespoke Tailoring

24.5 Ultimately, the responsibility for internet safety and the configuration of filtering lies with the Principal with support from SLT and DSL (the filtering solution can be tailored to meet the needs of individual schools if required) as administered by the IT Support Team (see Appendix 5).

Monitoring and Reporting

- 24.6 Internet traffic monitoring will be regularly undertaken by site IT Teams and reviews of filtering capabilities and categories will be conducted in line with reviews to this policy and government legislation.
- 24.7 The Trust/its Academies have a clearly defined procedure for reporting breaches or failures in filtering. All staff and students will be aware of this procedure by reading the AUP and by receiving the appropriate awareness training.
- 24.8 If users discover a website with inappropriate or potentially illegal content, this should be reported to a member of staff who will inform the Designated Safeguarding Lead and the relevant IT Team. All incidents should be documented and, if necessary, reported to appropriate agencies.
- 24.9 Although staff will monitor students' use of the internet in lessons, there will be a degree of independence when completing work using the internet.

25. EMAIL

- 25.1 LEAP MAT provides each student and member of staff a Microsoft Office 365 email account which should be limited in its use for **educational and work-based purposes**. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal information being revealed. LEAP MAT does, however, consider individual email accounts to be personal data, but will be monitored and accessed under certain circumstances, such as safeguarding or for disciplinary proceedings. Any email account access in these circumstances will be authorised by SLT/DSL.
- 25.2 All communication between staff and parents and carers and students must be professional in tone and content and **recipients** should be written and checked carefully before sending. These communications must adhere to LEAP MAT GDPR policies and be facilitated via their Office 365 email service. They must not be sent from personal e-mail addresses of staff, via text messaging or any public chat or social networking programme.
- 25.3 Academies use a standard disclaimer attached to all external email correspondence.

Usage

- 25.4 All email and attachments are scanned for viruses, malicious content and inappropriate messages. Any inappropriate use, or inappropriate messages from within LEAP MAT or an external source should report to a member of staff or SLT immediately.
- 25.5 Irrespective of how staff and students access their school email account, this policy and the AUP still applies.

Accessing via Mobile Devices

- 25.6 Office365 email accounts can be accessed via mobile devices either via mail applications or directly via a web interface.
- 25.7 When using a mail application such as Microsoft Outlook, users must agree to the LEAP MAT Mobile Device Management policy. This policy ensures that data is protected by applying the correct security settings (strong access passcodes and PINs) to the enrolled device, and that in certain exceptional circumstances (such as the loss of a device) the device can be remotely accessed and e-mail data erased.

Rules

- 25.8 The Trust/Academies will apply automatic external message monitoring, filtering and rejection systems as appropriate, and deny transmission of messages with content that is deemed unacceptable. These monitoring arrangements will operate on a continual and continuing basis with the express aim of monitoring compliance with the provisions of this policy and IT Regulations and for the purposes as permitted by The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.
- 25.9 Individual Principals can tailor e-mail rules to suit, but the LEAP MAT baseline rules are as follows:
- **SIXTH FORM STUDENTS (KS5):** KS5 students are allowed to email staff and moderated external organisations such as UCAS and Universities and Colleges
 - **KEY STAGE 3 AND 4 STUDENTS (KS3/4):** KS3/4 students are allowed to email staff, but are not allowed to e-mail any other student or any external organisations
- 25.10 LEAP MAT has adopted the Parents and Teachers for Excellence (PTE) campaign to support mobile device free schools.

The principle to limit screen time during school hours means for Year 7-11 students, mobile devices are not to be used, seen, or heard at any point, anywhere on the school site. Mobile phones should be concealed and switched off before entering school gates.

Breaches of this rule, without expressed permission in exceptional circumstances, will be sanctioned in the line with Trust's Behaviour Policy.

It is essential that students adhere to this rule and ensure that they **do not have phones, devices, including smart watches, on their person as they enter examination rooms.** This is a JCQ examination rule and if breached, a student risks disqualification from the exam/series of exams.

If a student needs to contact his/her parents or carers in an emergency during the school day, they will be allowed to use a school phone.

Students are made aware that sending or sharing sexual images/ content will not be tolerated as these actions are illegal (see section 12 about peer-on-peer abuse & online sexual abuse).

Students must not photograph, record images/voices of students or staff without permission at ANYTIME.

If a student breaches the Academy policy then the phone or device will be confiscated and will be held in a secure place eg in the school office. Mobile phones and devices are usually released at the end of the school day, however, students may be sanctioned in line with the Trust's Behaviour Policy for defiance to staff and repeated failure to respect school rules.

(See section about bring your own device BYOD below- section 28)

Phones and devices must not be taken into examinations. It is essential that students adhere to this rule and ensure that they do not have phones, devices, including smart watches, on their person as they enter examination rooms. This is

a JCQ examination rule and if breached, a student risks disqualification from the exam/series of exams.

If a student needs to contact his/her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

- **STAFF** - Where staff are required to use a mobile phone for Trust duties, for instance in case of emergency during off-site activities/visits, or for contacting students or parents, then a Trust device will be provided.

In some exceptional circumstances, or when a member of staff does not have access to a school device, they are permitted to use their own mobile phone but should mask/hide their own number for data privacy purposes.

Staff are encouraged not to use personal devices to connect to the school's Wi-Fi infrastructure, but are allowed to if they request it. Staff must adhere to this policy and the AUP and no personal device will be permitted to use a wired connection to any of the LEAP MAT or school's infrastructure. See also: BYOD policy

26. DATA PROTECTION AND INFORMATION SECURITY

26.1 LEAP MAT will act and carry out its duty of care for the digital information it holds in line with the Data Protection Act 2018 – the UK's implementation of the General Data Protection Regulation (GDPR).

26.2 Office 365 data is stored in accordance with EU-US Privacy Shield Framework (replacing the Safe Harbor Framework) that provides a mechanism to comply with data protection requirements when transferring data between the European Union and the United States.
See also: GDPR Policy

27. MANAGEMENT OF ASSETS

27.1 IT store PC hardware/software in System Center. IT assets below the value of £250 won't be recorded.

All redundant ICT equipment will be disposed of through an authorised agency.

All redundant ICT equipment that may have held personal data will have the storage media erased.

Disposal of any ICT equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007.

28. BRING YOUR OWN DEVICE (BYOD) - INTRODUCTION

This supplements section 25.10 above, where Principals recognise the benefits to learning from offering students the opportunity to use personal devices in school (Bring Your Own Device – BYOD) to support educational activities as an exception to the use of mobile devices as described in section 25.10

28.1 BYOD – wi-fi provision

Whilst we recognise that using personal devices can enhance directed learning, we also recognise the need to protect students from offensive and dangerous material and acknowledge the need to ensure all users make responsible use of the

internet. Internet access will be granted via a voucher system, and limited and filtered in compliance with Government guidelines. See Appendix 5 – Internet Settings.

28.2 **BYOD – classroom usage**

When explicitly permitted by a member of staff a personal device may be used in lesson to support the lesson objectives. This could be note taking, or for broader learning during independent study. Using a device for any other reason other than directed, for example games, is not allowed. If a device is hidden (e.g. under a table, or shielded from an approaching teacher) staff will assume inappropriate use and confiscate the device.

28.3 **BYOD – independent study**

Key Stage 5 students can use their own devices to support educational activities in nominated private study rooms, supervised study lessons or the sixth form common room.

28.4 **BYOD – additional acceptable use policy**

If students use personal devices to connect to the school provided BYOD network, then they must agree to be bound by the additional rules set out in the BYOD Acceptable Use Policy.

28.5 **BYOD – device security & management**

BYOD is in addition to the curriculum and is not a compulsory element of a student's education. It is not the school's responsibility to provide or support personal devices. The purchase, maintenance, safety, insurance and security of all personal devices must be borne by parents/students. All personally-owned devices brought to school are the responsibility of the device owner. The Academy accepts no responsibility for the loss, theft or damage of personally-owned devices.

There are no secure facilities provided at school to store personal devices. Students should therefore keep their personal devices with them at all times.

28.6 **BYOD – misuse**

Illegal and inappropriate use of ICT services will not be tolerated. Students may face disciplinary action if they engage in any such activities, including Cyber-bullying and bypassing internet filtering, or the use of electronic communication to harass, abuse or radicalise others. If there is a reason to believe that a student has violated school policy or engaged in misconduct whilst using their device, then evidence will be obtained removed from that device. See section 19.1-5 above, Removing Evidence from Digital Devices. (NB see 19.2 - images/content thought to be of a sexual nature must NOT be removed and stored on the school system – this is illegal).

Access to the school provided BYOD network is a privilege, not a right and can be withdrawn at any time.

28.7 **Student bring-your-own device acceptable use policy (BYOD-AUP)**

You must adhere to the LEAP MAT Data Protection and Privacy policies, Safeguarding Policy, Student Acceptable Use Policy (AUP) and the following Bring Your Own Device Acceptable Use Policy (BYOD-AUP) when using your own personal device in school:

- You are expected to be a responsible user of ICT. Illegal and inappropriate use of ICT services will not be tolerated. You may face disciplinary action if you engage in any such activities. These include, without limitation; cyber-bullying and online abuse; attempting to hack the security of, access or tamper with any parts of the Wi-Fi service; attempting to circumvent the internet

filtering service – this includes setting up proxies or using programs to bypass firewall securities; calling, texting, emailing, or communication with any others from a personal device, including other students, parents, guardians, friend and family during school time; or taking, recording or distributing pictures, video or any other material relating to students, staff or areas of the school. (See Safeguarding policy, sections 17-19 about Misuse and Removing Evidence from Digital Devices).

- During directed learning where devices are allowed, **connections to the internet must be via the school provided Wi-Fi only**. Unfiltered personal data connections must not be used.
- Where directed by staff, you may use a device to take pictures, or record video or other material relating to educational activities. You must install the OneDrive app on your device and use your school provided Office365 account to store this material on your device. Media must not be saved outside the OneDrive mechanism on personal device camera-rolls or internal storage. You are not permitted to use personal devices for storage of any images, video or sound clips of students/staff. (See Safeguarding Policy section 20 about storage of content)
- There are no secure facilities provided at school to store personal devices. You should therefore keep your devices with you at all times.
- You bring your device to school at your own risk. It is your duty to act responsibly with regard to that device. The Academy is not responsible for personal devices that are broken, lost or stolen whilst at school; any data that is lost on personal devices whilst in school; or maintenance, support, troubleshooting or upkeep or any personal device whilst in school.
- You must ensure that your device has a suitable protective case and has adequate insurance in place to cover the cost of replacement or repair in the event of loss or damage.
- To mitigate data loss or misuse, where possible your device should have the appropriate PIN, biometric or suitable device lock and be backed up regularly. Tracking apps such as Find My Device or Find My iPhone should be installed and activated.
- You must take all reasonable steps to prevent transmission or receipt of malicious software, such as computer viruses or malware. (See Safeguarding policy section 16-Preventing the spread of malicious software (Malware, viruses and cryptoware))
- You are responsible for charging your personal devices prior to bringing them into school. If USB charging outlets are provided then they can be used. **You must not connect any personal devices and chargers to school power outlets or connect them via cable to school computers.**
- If you have been allowed to listen to audio files such as music then the volume must be kept at a level that does not disrupt others.

FREQUENTLY ASKED QUESTIONS

1. What devices are permitted or recommended?
Smartphones, tablets and lightweight laptops such as Chromebooks.

2. How do I get permission to use BYOD?
Read and agree to the terms of the AUP and BYOD-AUP and see your Head of Year /subject teacher for a voucher code.
3. Can I transfer work from school computers to my personal device and vice-versa?
You can transfer work to and from school by using OneDrive in your school provided Office365 account, or via other school approved means such as the Satchel One (Show My Homework) app. No other method or storage should be used, such as external USB drives.
4. Can I connect my device to a school PC?
No, you are not permitted to connect a personal device via a wire to any school PC or wired network socket.
5. Can I print to school printers from my device?
No.
6. Can I use my personal device in class?
Devices may only be used in class with the approval and direction of the class teacher, otherwise all personal devices must be switched off and kept out of sight.

29. RELEVANT POLICIES

- 29.1 To underpin the values and ethos of our Academy and our intent to ensure that students at our Academy are appropriately safeguarded the following policies are also included under our safeguarding umbrella:-
- LEAP Staff Safeguarding Code of Conduct
 - LEAP Anti-Bullying Policy
 - LEAP Behaviour Policy
 - LEAP Use of force to control or restrain students
 - LEAP Attendance Policy
 - LEAP Health and Safety including site security
 - LEAP Equality Strategy
 - LEAP Supporting students with medical needs policy
 - LEAP Educational Visits
 - LEAP Whistleblowing policy
 - LEAP Staff and Student Acceptable Use Agreements
 - LEAP Information Technology Security Document
 - LEAP GDPR Data Protection Policy
 - LEAP GDPR working practices document

30. STATUTORY FRAMEWORK

- 30.1 This policy has been devised in accordance with the following legislation and guidance:-
- *'Working Together to Safeguard Children* DfE (2018), updated December 2020
 - *'Keeping Children Safe in Education'*, DfE (2021)
 - Guidance for Safer Working Practices for Adults who work with Children and Young People (May 2019, Safer Recruitment Consortium, Addendum April 2020)
- <https://rotherhamscb.proceduresonline.com>

Appendix 1: Making a Referral to Children's Social Care

A telephone referral should be made in the following circumstances to Starting Point Derbyshire 01629 535353 or refer to www.derbyshire.gov.uk/socialhealth/children-and-families/support-for-families/startingpointreferral

- A child or young person makes a clear allegation of abuse
- A child has been abandoned
- Further concerns have arisen in relation to an open case to Children's Social Care
- Concerns of significant harm have risen for a child receiving a service as a **Child in Need**
- Further concerns have arisen of increased or additional risk to a child currently subject to a **Child Protection Plan**
- A child sustains an injury and there is professional concern about how it was caused
- There are any circumstances which suggest that a child is suffering or is likely to suffer **Significant Harm**
- An unborn child may be at risk of significant harm – for more information see **Safeguarding Unborn and Newborn Babies Procedure** and **Concealment and Denial of Pregnancy Procedure**
- A non-mobile infant sustains any injury, however slight, **without an adequate accidental explanation**
- A member of the public makes an allegation that someone has abused a child
- Professional concern exists about abuse or neglect, despite no allegation being made
- A child has been made the subject of an Emergency Protection Order or a **Police Protection Order**
- Concerns have arisen for a child who is the subject of a **Supervision Order** or Care Order
- Despite professional intervention, either on a single agency basis or as part of early help intervention, because of suspected neglect or abuse there is concern that a child is suffering or is likely to suffer significant harm or requires additional support – see **Practice Guidance: Significant Harm - The Impact of Abuse and Neglect** for more information
- There are concerns that a child or young person is being sexually exploited - for more information see **Action Following Referral of Safeguarding Children Concerns Procedure, Child Sexual Exploitation (CSE)** and **Safeguarding Children and Young People from Sexual Exploitation Procedure**
- A child is reported missing from home or care and there are additional concerns about their vulnerability – for more information see **Safeguarding Children and Young People who go Missing from Home and Care**
- There are concerns a child may be harmed because of use of technology or social media – for more information see **E-Safety: Safeguarding Children Exposed to Harm through the Digital Media**
- Concern exists about a child having contact with a person who may pose a risk, or potential risk, to children (see **Individuals who Pose a Risk to Children Procedure**)
- A child is being denied access to urgent or important **Medical Assessment** or services
- There are suspicions that a child might be harmed because of fabricated or induced illness (see **Protocol for Safeguarding Children in Whom Illness is Fabricated or Induced**)
- A child is at risk of being subjected to illegal procedures, for example:-

- **Safeguarding Girls and Young Women at Risk of Abuse through Female Genital Mutilation Procedure**
- **Safeguarding Children and Young People from Forced Marriage Procedure**
- **Safeguarding Children and Young People from Honour Based Violence Procedure**
- There are grounds for concern that a person may be a victim of human trafficking (see **Safeguarding Children who may have been Trafficked from Abroad Procedure** and **National Referral Mechanism: guidance for child first responders (Home Office, August 2013)**)
- A child is at risk or vulnerable to being drawn into terrorism - for more information see **Supporting Children and Young People Vulnerable to Violent Extremism Procedure**
- A child is at risk of being harmed through experiencing or seeing or hearing the ill-treatment of another, e.g. through **Domestic Abuse**
- A child is at risk of being harmed because of concerns about their parents' mental health see - **Safeguarding Children at Risk where a Parent has Mental Health Problem Procedure**
- Either an adult or a child makes allegations of non-recent abuse, for more information see - **Safeguarding Children and Young People Involved in Organised or Multiple Abuse, and other Complex Investigations Procedure.**

For information about thresholds, see **Multi-Agency Threshold Descriptors.**

Please note this list is not exhaustive.

Useful Contact numbers and e-mail addresses/websites:-

Derbyshire Starting Point 01629 533190
Derbyshire LADO 0133 641172

Sheffield safeguarding hub 0114 2734855
<https://www.safeguardingsheffieldchildren.org/sscb/safeguarding-information-and-resources/referring-a-safeguarding-concern-to-childrens-social-care>

National Helplines/Websites:

NSPCC Confidential helpline – 0808 800 5000
help@nspcc.org.uk

Childline – 0800 1111

Remove a nude image shared online:

<https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/remove-nude-image-shared-online/>

Appendix 2: Categories of Abuse and Neglect and other safeguarding issues

This information is taken from KCSE 2021: Part one – for ALL staff

26. **Abuse:** a form of maltreatment of a child. Somebody may abuse or neglect a child by inflicting harm or by failing to act to prevent harm. Children may be abused in a family or in an institutional or community setting by those known to them or, more rarely, by others. Abuse can take place wholly online, or technology may be used to facilitate offline abuse. Children may be abused by an adult or adults or by another child or children.

27. **Physical abuse:** a form of abuse which may involve hitting, shaking, throwing, poisoning, burning or scalding, drowning, suffocating or otherwise causing physical harm to a child. Physical harm may also be caused when a parent or carer fabricates the symptoms of, or deliberately induces, illness in a child.

28. **Emotional abuse:** the persistent emotional maltreatment of a child such as to cause severe and adverse effects on the child's emotional development. It may involve conveying to a child that they are worthless or unloved, inadequate, or valued only insofar as they meet the needs of another person. It may include not giving the child opportunities to express their views, deliberately silencing them or 'making fun' of what they say or how they communicate. It may feature age or developmentally inappropriate expectations being imposed on children. These may include interactions that are beyond a child's developmental capability as well as overprotection and limitation of exploration and learning or preventing the child from participating in normal social interaction. It may involve seeing or hearing the ill-treatment of another. It may involve serious bullying (including cyberbullying), causing children frequently to feel frightened or in danger, or the exploitation or corruption of children. Some level of emotional abuse is involved in all types of maltreatment of a child, although it may occur alone.

29. **Sexual abuse:** involves forcing or enticing a child or young person to take part in sexual activities, not necessarily involving violence, whether or not the child is aware of what is happening. The activities may involve physical contact, including assault by penetration (for example rape or oral sex) or non-penetrative acts such as masturbation, kissing, rubbing, and touching outside of clothing.

They may also include non-contact activities, such as involving children in looking at, or in the production of, sexual images, watching sexual activities, encouraging children to behave in sexually inappropriate ways, or grooming a child in preparation for abuse. Sexual abuse can take place online, and technology can be used to facilitate offline abuse. Sexual abuse is not solely perpetrated by adult males. Women can also commit acts of sexual abuse, as can other children. The sexual abuse of children by other children is a specific safeguarding issue (also known as peer on peer abuse) in education and all staff should be aware of it and of their school policy and procedures for dealing with it, (see paragraph 49).

30. **Neglect:** the persistent failure to meet a child's basic physical and/or psychological needs, likely to result in the serious impairment of the child's health or development. Neglect may occur during pregnancy, for example, as a result of maternal substance abuse. Once a child is born, neglect may involve a parent or carer failing to: provide adequate food, clothing and shelter (including exclusion from home or abandonment); protect a child from physical and emotional harm or danger; ensure adequate supervision (including the use of inadequate care-givers); or ensure access to

appropriate medical care or treatment. It may also include neglect of, or unresponsiveness to, a child's basic emotional needs.

Safeguarding issues

31. All staff should have an awareness of safeguarding issues that can put children at risk of harm. Behaviours linked to issues such as drug taking and or alcohol misuse, deliberately missing education and consensual and non-consensual sharing of nudes and semi-nudes images and/or videos can be signs that children are at risk. Other safeguarding issues all staff should be aware of include:

Child Sexual Exploitation (CSE) and Child Criminal Exploitation (CCE)

32. Both CSE and CCE are forms of abuse that occur where an individual or group takes advantage of an imbalance in power to coerce, manipulate or deceive a child into taking part in sexual or criminal activity, in exchange for something the victim needs or wants, and/or for the financial advantage or increased status of the perpetrator or facilitator and/or through violence or the threat of violence. CSE and CCE can affect children, both male and female and can include children who have been moved (commonly referred to as trafficking) for the purpose of exploitation.

Child Criminal Exploitation (CCE)

33. Some specific forms of CCE can include children being forced or manipulated into transporting drugs or money through county lines, working in cannabis factories, shoplifting or pickpocketing. They can also be forced or manipulated into committing vehicle crime or threatening/committing serious violence to others.

34. Children can become trapped by this type of exploitation as perpetrators can threaten victims (and their families) with violence, or entrap and coerce them into debt. They may be coerced into carrying weapons such as knives or begin to carry a knife for a sense of protection from harm from others. As children involved in criminal exploitation often commit crimes themselves, their vulnerability as victims is not always recognised by adults and professionals, (particularly older children), and they are not treated as victims despite the harm they have experienced. They may still have been criminally exploited even if the activity appears to be something they have agreed or consented to.

35. It is important to note that the experience of girls who are criminally exploited can be very different to that of boys. The indicators may not be the same, however professionals should be aware that girls are at risk of criminal exploitation too. It is also important to note that both boys and girls being criminally exploited may be at higher risk of sexual exploitation.

Further information about CCE including definitions and indicators is included in Annex B.

Child Sexual Exploitation (CSE)

36. CSE is a form of child sexual abuse. Sexual abuse may involve physical contact, including assault by penetration (for example, rape or oral sex) or nonpenetrative acts such as masturbation, kissing, rubbing, and touching outside clothing. It may include noncontact activities, such as involving children in the production of sexual images, forcing children to look at sexual images or watch sexual activities, encouraging children to behave in sexually inappropriate ways or grooming a child in preparation for abuse including via the internet.

37. CSE can occur over time or be a one-off occurrence, and may happen without the child's immediate knowledge e.g. through others sharing videos or images of them on social media.

38. CSE can affect any child, who has been coerced into engaging in sexual activities. This includes 16 and 17 year olds who can legally consent to have sex. Some children may not realise they are being exploited e.g. they believe they are in a genuine romantic relationship.

39. Further information about CSE including definitions and indicators is included in Annex B.

Female Genital Mutilation (FGM)

40. Whilst all staff should speak to the designated safeguarding lead (or deputy) with regard to any concerns about female genital mutilation (FGM), there is a specific legal duty on teachers. If a teacher, in the course of their work in the profession, discovers that an act of FGM appears to have been carried out on a girl under the age of 18, the teacher must report this to the police. See Annex B for further details.

Mental Health

41. All staff should be aware that mental health problems can, in some cases, be an indicator that a child has suffered or is at risk of suffering abuse, neglect or exploitation.

42. Only appropriately trained professionals should attempt to make a diagnosis of a mental health problem. Education staff, however, are well placed to observe children day-to-day and identify those whose behaviour suggests that they may be experiencing a mental health problem or be at risk of developing one.

43. Where children have suffered abuse and neglect, or other potentially traumatic adverse childhood experiences, this can have a lasting impact throughout childhood, adolescence and into adulthood. It is key that staff are aware of how these children's experiences, can impact on their mental health, behaviour, and education.

44. Schools and colleges can access a range of advice to help them identify children in need of extra mental health support, this includes working with external agencies. More information can be found in the mental health and behaviour in schools' guidance, colleges may also wish to follow this guidance as best practice. Public Health England has produced a range of resources to support secondary school teachers to promote positive health, wellbeing and resilience among children. See Rise Above for links to all materials and lesson plans.

45. If staff have a mental health concern about a child that is also a safeguarding concern, immediate action should be taken, following their child protection policy, and speaking to the designated safeguarding lead or a deputy.

Peer on peer abuse (child on child)

46. All staff should be aware that children can abuse other children (often referred to as peer on peer abuse). And that it can happen both inside and outside of school or college and online. It is important that all staff recognise the indicators and signs of peer on peer abuse and know how to identify it and respond to reports.

47. All staff should understand, that even if there are no reports in their schools or colleges it does not mean it is not happening, it may be the case that it is just not being reported. As such it is important if staff have any concerns regarding peer on peer abuse they should speak to their designated safeguarding lead (or deputy).

48. It is essential that all staff understand the importance of challenging inappropriate behaviours between peers, many of which are listed below, that are actually abusive in nature. Downplaying certain behaviours, for example dismissing sexual harassment as "just banter", "just having a laugh", "part of growing up" or "boys being boys" can lead to a culture of unacceptable behaviours, an unsafe environment for children and in worst

case scenarios a culture that normalises abuse leading to children accepting it as normal and not coming forward to report it.

49. Peer on peer abuse is most likely to include, but may not be limited to:

- bullying (including cyberbullying, prejudice-based and discriminatory bullying);
- abuse in intimate personal relationships between peers.
- physical abuse such as hitting, kicking, shaking, biting, hair pulling, or otherwise causing physical harm (this may include an online element which facilitates, threatens and/or encourages physical abuse).
- sexual violence, such as rape, assault by penetration and sexual assault; (this may include an online element which facilitates, threatens and/or encourages sexual violence).
- sexual harassment, such as sexual comments, remarks, jokes and online sexual harassment, which may be standalone or part of a broader pattern of abuse.
- causing someone to engage in sexual activity without consent, such as forcing someone to strip, touch themselves sexually, or to engage in sexual activity with a third party.
- consensual and non-consensual sharing of nudes and semi nudes images and or videos (also known as sexting or youth produced sexual imagery);
- upskirting, which typically involves taking a picture under a person’s clothing without their permission, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm; and
- initiation/hazing type violence and rituals (this could include activities involving harassment, abuse or humiliation used as a way of initiating a person into a group and may also include an online element).

50. All staff should be clear as to the school’s or college’s policy and procedures with regards to peer on peer abuse and the important role they have to play in preventing it and responding where they believe a child may be at risk from it.

Serious violence

51. All staff should be aware of the indicators, which may signal children are at risk from, or are involved with serious violent crime. These may include increased absence from school, a change in friendships or relationships with older individuals or groups, a significant decline in performance, signs of self-harm or a significant change in wellbeing, or signs of assault or unexplained injuries. Unexplained gifts or new possessions could also indicate that children have been approached by, or are involved with, individuals associated with criminal networks or gangs and may be at risk of criminal exploitation (see paragraphs 33-35).

52. All staff should be aware of the range of risk factors which increase the likelihood of involvement in serious violence, such as being male, having been frequently absent or permanently excluded from school, having experienced child maltreatment and having been involved in offending, such as theft or robbery. Advice for schools and colleges is provided in the Home Office’s [Preventing youth violence and gang involvement](#) and its [Criminal exploitation of children and vulnerable adults: county lines](#) guidance.

Appendix 3: Further Information on Specific Concerns (Annexe B KCSE 2021)

Child abduction and community safety incidents

Child abduction is the unauthorised removal or retention of a minor from a parent or anyone with legal responsibility for the child. Child abduction can be committed by parents or other family members; by people known but not related to the victim (such as neighbours, friends and acquaintances); and by strangers.

Other community safety incidents in the vicinity of a school can raise concerns amongst children and parents, for example, people loitering nearby or unknown adults engaging children in conversation.

As children get older and are granted more independence (for example, as they start walking to school on their own) it is important they are given practical advice on how to keep themselves safe. Many schools provide outdoor-safety lessons run by teachers or by local police staff.

It is important that lessons focus on building children's confidence and abilities rather than simply warning them about all strangers. Further information is available at: www.actionagainstabduction.org and www.clevernevergoes.org.

Children and the court system

Children are sometimes required to give evidence in criminal courts, either for crimes committed against them or for crimes they have witnessed. There are two age appropriate guides to support children 5-11-year olds and 12-17 year olds.

The guides explain each step of the process, support and special measures that are available. There are diagrams illustrating the courtroom structure and the use of video links is explained.

Making child arrangements via the family courts following separation can be stressful and entrench conflict in families. This can be stressful for children. The Ministry of Justice has launched an online child arrangements information tool with clear and concise information on the dispute resolution service. This may be useful for some parents and carers.

Children missing from education

All staff should be aware that children going missing, particularly repeatedly, can act as a vital warning sign of a range of safeguarding possibilities. This may include abuse and neglect, which may include sexual abuse or exploitation and can also be a sign of child criminal exploitation including involvement in county lines. It may indicate mental health problems, risk of substance abuse, risk of travelling to conflict zones, risk of female genital mutilation or risk of forced marriage. Early intervention is necessary to identify the existence of any underlying safeguarding risk and to help prevent the risks of a child going missing in future. Staff should be aware of their school's or college's unauthorised absence and children missing from education procedures.

Children with family members in prison

Approximately 200,000 children in England and Wales have a parent sent to prison each year. These children are at risk of poor outcomes including poverty, stigma, isolation and poor mental health. NICCO provides information designed to support professionals working with offenders and their children, to help mitigate negative consequences for those children.

Child Criminal Exploitation (CCE) and Child Sexual Exploitation (CSE)

We know that different forms of harm often overlap, and that perpetrators may subject children and young people to multiple forms of abuse, such as criminal exploitation (including county lines) and sexual exploitation.

In some cases, the exploitation or abuse will be in exchange for something the victim needs or wants (for example, money, gifts or affection), and/or will be to the financial benefit or other advantage, such as increased status, of the perpetrator or facilitator.

Children can be exploited by adult males or females, as individuals or in groups. They may also be exploited by other children, who themselves may be experiencing exploitation – where this is the case, it is important that the child perpetrator is also recognised as a victim.

Whilst the age of the child may be a contributing factor for an imbalance of power, there are a range of other factors that could make a child more vulnerable to exploitation, including gender, sexual identity, cognitive ability, learning difficulties, communication ability, physical strength, status, and access to economic or other resources.

Some of the following can be indicators of both child criminal and sexual exploitation where children:

- appear with unexplained gifts, money or new possessions.
- associate with other children involved in exploitation.
- suffer from changes in emotional well-being; misuse drugs and alcohol.
- go missing for periods of time or regularly come home late; and
- regularly miss school or education or do not take part in education.

Children who have been exploited will need additional support to help maintain them in education.

CSE can be a one-off occurrence or a series of incidents over time and range from opportunistic to complex organised abuse. It can involve force and/or enticement-based methods of compliance and may, or may not, be accompanied by violence or threats of violence.

Some additional specific indicators that may be present in CSE are children who:

- have older boyfriends or girlfriends; and
- suffer from sexually transmitted infections, display sexual behaviours beyond expected sexual development or become pregnant.

Further information on signs of a child's involvement in sexual exploitation is available in the Home Office guidance: [Child sexual exploitation: guide for practitioners](#)

County lines

County lines is a term used to describe gangs and organised criminal networks involved in exporting illegal drugs using dedicated mobile phone lines or other form of “deal line”. This activity can happen locally as well as across the UK - no specified distance of travel is required. Children and vulnerable adults are exploited to move, store and sell drugs and money. Offenders will often use coercion, intimidation, violence (including sexual violence) and weapons to ensure compliance of victims.

Children can be targeted and recruited into county lines in a number of locations including schools (mainstream and special), further and higher educational institutions, pupil referral units, children's homes and care homes.

Children are also increasingly being targeted and recruited online using social media. Children can easily become trapped by this type of exploitation as county lines gangs can manufacture drug debts which need to be worked off or threaten serious violence and kidnap towards victims (and their families) if they attempt to leave the county lines network.

A number of the indicators for CSE and CCE as detailed above may be applicable to where children are involved in county lines. Some additional specific indicators that may be present where a child is criminally exploited through involvement in county lines are children who:

- go missing and are subsequently found in areas away from their home.
- have been the victim or perpetrator of serious violence (e.g. knife crime);
- are involved in receiving requests for drugs via a phone line, moving drugs, handing over and collecting money for drugs.
- are exposed to techniques such as 'plugging', where drugs are concealed internally to avoid detection.
- are found in accommodation that they have no connection with, often called a 'traphouse or cuckooing' or hotel room where there is drug activity.
- owe a 'debt bond' to their exploiters.
- have their bank accounts used to facilitate drug dealing.

Further information on the signs of a child's involvement in county lines is available in guidance published by the [Home Office](#).

Cybercrime

Cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that can happen off-line but are enabled at scale and at speed on-line) or 'cyber dependent' (crimes that can be committed only by using a computer). Cyber-dependent crimes include:

- unauthorised access to computers (illegal 'hacking'), for example accessing a school's computer network to look for test paper answers or change grades awarded.
- denial of Service (Dos or DDoS) attacks or 'booting'. These are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources; and,
- making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above.

Children with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime.

If there are concerns about a child in this area, the designated safeguarding lead (or a deputy), should consider referring into the **Cyber Choices** programme. This is a nationwide police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests.

Note that **Cyber Choices** does not currently cover 'cyber-enabled' crime such as fraud, purchasing of illegal drugs on-line and child sexual abuse and exploitation, nor other areas of concern such as on-line bullying or general on-line safety.

Modern Slavery and the National Referral Mechanism

Modern slavery encompasses human trafficking and slavery, servitude and forced or compulsory labour. Exploitation can take many forms, including: sexual exploitation, forced labour, slavery, servitude, forced criminality and the removal of organs.

Further information on the signs that someone may be a victim of modern slavery, the support available to victims and how to refer them to the NRM is available in the Modern Slavery Statutory Guidance

Domestic abuse

The cross-government definition of domestic violence and abuse is: any incident or pattern of incidents of controlling, coercive, threatening behaviour, violence or abuse between those aged 16 or over who are, or have been, intimate partners or family members regardless of gender or sexuality. The abuse can encompass, but is not limited to: psychological; physical; sexual; financial; and emotional.

All children can witness and be adversely affected by domestic abuse in the context of their home life where domestic abuse occurs between family members. Exposure to domestic abuse and/or violence can have a serious, long lasting emotional and psychological impact on children. In some cases, a child may blame themselves for the abuse or may have had to leave the family home as a result.

Operation Encompass

Operation Encompass operates in the majority of police forces across England. It helps police and schools work together to provide emotional and practical help to children. The system ensures that when police are called to an incident of domestic abuse, where there are children in the household who have experienced the domestic incident, the police will inform the key adult (usually the designated safeguarding lead) in school before the child or children arrive at school the following day. This ensures that the school has up to date relevant information about the child's circumstances and can enable support to be given to the child according to their needs. Police forces not signed up to operation encompass will have their own arrangements in place.

National Domestic Abuse Helpline

Refuge runs the National Domestic Abuse Helpline, which can be called free of charge and in confidence, 24 hours a day on 0808 2000 247. Its website provides guidance and support for potential victims, as well as those who are worried about friends and loved ones. It also has a form through which a safe time from the team for a call can be booked.

Additional advice on identifying children who are affected by domestic abuse and how they can be helped is available at:

- NSPCC- UK domestic-abuse Signs Symptoms Effects
- Refuge what is domestic violence/effects of domestic violence on children
- SafeLives: young people and domestic abuse.

Homelessness

Being homeless or being at risk of becoming homeless presents a real risk to a child's welfare. The designated safeguarding lead (and any deputies) should be aware of contact details and referral routes in to the Local Housing Authority so they can raise/progress concerns at the earliest opportunity. Indicators that a family may be at risk of homelessness include household debt, rent arrears, domestic abuse and anti-social behaviour, as well as the family being asked to leave a property. Whilst referrals and/or discussion with the Local Housing Authority should be progressed as appropriate, and in accordance with local procedures, this does not, and should not, replace a referral into children's social care where a child has been harmed or is at risk of harm.

The Homelessness Reduction Act 2017 places a new legal duty on English councils so that everyone who is homeless or at risk of homelessness will have access to meaningful help including an assessment of their needs and circumstances, the development of a personalised housing plan, and work to help them retain their accommodation or find a new place to live. The following factsheets usefully summarise the new duties: Homeless Reduction Act Factsheets. The new duties shift focus to early intervention and encourage those at risk to seek support as soon as possible, before they are facing a homelessness crisis.

In most cases school and college staff will be considering homelessness in the context of children who live with their families, and intervention will be on that basis. However, it should also be recognised in some cases 16 and 17 year olds could be living independently from their parents or guardians, for example through their exclusion from the family home, and will require a different level of intervention and support. Children's services will be the lead agency for these young people and the designated safeguarding lead (or a deputy) should ensure appropriate referrals are made based on the child's circumstances. The department and the Ministry of Housing, Communities and Local Government have published joint statutory guidance on the provision of accommodation for 16 and 17 year olds who may be homeless and/or require accommodation.

So-called 'honour-based' abuse (including Female Genital Mutilation and Forced Marriage)

So-called 'honour-based' abuse (HBA) encompasses incidents or crimes which have been committed to protect or defend the honour of the family and/or the community, including female genital mutilation (FGM), forced marriage, and practices such as breast ironing. Abuse committed in the context of preserving "honour" often involves a wider network of family or community pressure and can include multiple perpetrators.

It is important to be aware of this dynamic and additional risk factors when deciding what form of safeguarding action to take. All forms of HBA are abuse (regardless of the motivation) and should be handled and escalated as such. Professionals in all agencies, and individuals and groups in relevant communities, need to be alert to the possibility of a child being at risk of HBA, or already having suffered HBA.

Actions

If staff have a concern regarding a child that might be at risk of HBA or who has suffered from HBA, they should speak to the designated safeguarding lead (or deputy). As appropriate, they will activate local safeguarding procedures, using existing national and local protocols for multi-agency liaison with police and children's social care. Where FGM has taken place, since 31 October 2015 there has been a mandatory reporting duty placed on teachers¹⁰⁴ that requires a different approach (see following section).

FGM

FGM comprises all procedures involving partial or total removal of the external female genitalia or other injury to the female genital organs. It is illegal in the UK and a form of child abuse with long-lasting harmful consequences.

FGM mandatory reporting duty for teachers

Section 5B of the Female Genital Mutilation Act 2003 (as inserted by section 74 of the Serious Crime Act 2015) places a statutory duty upon teachers along with regulated health and social care professionals in England and Wales, to report to the police where they discover (either through disclosure by the victim or visual evidence) that FGM appears to have been carried out on a girl under 18. Those failing to report such cases may face disciplinary sanctions. It will be rare for teachers to see visual evidence, and they should not be examining pupils or students, but the same definition of what is

meant by “to discover that an act of FGM appears to have been carried out” is used for all professionals to whom this mandatory reporting duty applies. Information on when and how to make a report can be found at: Mandatory reporting of female genital mutilation procedural information

Teachers must personally report to the police cases where they discover that an act of FGM appears to have been carried out.¹⁰⁵ Unless the teacher has good reason not to, they should still consider and discuss any such case with the school’s or college’s designated safeguarding lead (or deputy) and involve children’s social care as appropriate. The duty does not apply in relation to at risk or suspected cases (i.e. where the teacher does not discover that an act of FGM appears to have been carried out, either through disclosure by the victim or visual evidence) or in cases where the woman is 18 or over. In these cases, teachers should follow local safeguarding procedures.

Forced marriage

Forcing a person into a marriage is a crime in England and Wales. A forced marriage is one entered into without the full and free consent of one or both parties and where violence, threats or any other form of coercion is used to cause a person to enter into a marriage. Threats can be physical or emotional and psychological. A lack of full and free consent can be where a person does not consent or where they cannot consent (if they have learning disabilities, for example). Nevertheless, some perpetrators use perceived cultural practices as a way to coerce a person into marriage. Schools and colleges can play an important role in safeguarding children from forced marriage.

The Forced Marriage Unit has published statutory guidance and Multi-agency guidelines, pages 35-36 of which focus on the role of schools and colleges. School and college staff can contact the Forced Marriage Unit if they need advice or information: Contact: 020 7008 0151 or email fmufco.gov.uk.

Preventing radicalisation

Children are vulnerable to extremist ideology and radicalisation. Similar to protecting children from other forms of harms and abuse, protecting children from this risk should be a part of a schools’ or colleges’ safeguarding approach.

- **Extremism** is the vocal or active opposition to our fundamental values, including democracy, the rule of law, individual liberty and the mutual respect and tolerance of different faiths and beliefs. This also includes calling for the death of members of the armed forces.
- **Radicalisation** refers to the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups.
- **Terrorism** is an action that endangers or causes serious violence to a person/people; causes serious damage to property; or seriously interferes or disrupts an electronic system. The use or threat must be designed to influence the government or to intimidate the public and is made for the purpose of advancing a political, religious or ideological cause.

There is no single way of identifying whether a child is likely to be susceptible to an extremist ideology. Background factors combined with specific influences such as family and friends may contribute to a child’s vulnerability. Similarly, radicalisation can occur through many different methods (such as social media or the internet) and settings (such as within the home).

However, it is possible to protect vulnerable people from extremist ideology and intervene to prevent those at risk of radicalisation being radicalised. As with other safeguarding risks, staff should be alert to changes in children’s behaviour, which could

indicate that they may be in need of help or protection. Staff should use their judgement in identifying children who might be at risk of radicalisation and act proportionately which may include the designated safeguarding lead (or deputy) making a Prevent referral.

The school's or college's designated safeguarding lead (and any deputies) should be aware of local procedures for making a Prevent referral.

The Prevent Duty

All schools and colleges are subject to a duty under section 26 of the Counter Terrorism and Security Act 2015 (the CTSA 2015), in the exercise of their functions, to have "due regard to the need to prevent people from being drawn into terrorism".¹¹⁰

This duty is known as the Prevent duty.

The Prevent duty should be seen as part of schools' and colleges' wider safeguarding obligations. Designated safeguarding leads and other senior leaders should familiarise themselves with the revised Prevent duty guidance: for England and Wales, especially paragraphs 57-76, which are specifically concerned with schools (and also covers childcare). The guidance is set out in terms of four general themes: risk assessment, working in partnership, staff training, and IT policies.

There is additional guidance: Prevent duty guidance: for further education institutions in England and Wales that applies to colleges.

Channel

Channel is a voluntary, confidential support programme which focuses on providing support at an early stage to people who are identified as being vulnerable to being drawn into terrorism. Prevent referrals may be passed to a multi-agency Channel panel, which will discuss the individual referred to determine whether they are vulnerable to being drawn into terrorism and consider the appropriate support required. A representative from the school or college may be asked to attend the Channel panel to help with this assessment. An individual's engagement with the programme is entirely voluntary at all stages.

Guidance on Channel is available at: [Channel guidance](#).

Additional support

The department has published further advice for schools on the Prevent duty. The advice is intended to complement the Prevent guidance and signposts to other sources of advice and support. The Home Office has developed three e-learning modules:

- Prevent awareness e-learning offers an introduction to the Prevent duty.
- Prevent referrals e-learning supports staff to make Prevent referrals that are robust, informed and with good intention.
- Channel awareness e-learning is aimed at staff who may be asked to contribute to or sit on a multi-agency Channel panel.

Educate Against Hate, is a government website designed to support school teachers and leaders to help them safeguard their students from radicalisation and extremism. The platform provides free information and resources to help school staff identify and address the risks, as well as build resilience to radicalisation.

Peer on peer/ child on child abuse

Children can abuse other children (often referred to as peer on peer abuse) and it can take many forms. It **can** happen both inside and outside of school/college and online. It is important that all staff recognise the indicators and signs of peer on peer abuse and know how to identify it and respond to reports. This **can** include (but is not limited to): bullying (including cyberbullying, prejudice-based and discriminatory bullying); abuse within intimate partner relationships; physical abuse such as hitting, kicking, shaking, biting, hair pulling, or otherwise causing physical harm; sexual violence and sexual

harassment; consensual and non-consensual sharing of nudes and semi-nudes images and/or videos; causing someone to engage in sexual activity without consent, such as forcing someone to strip, touch themselves sexually, or to engage in sexual activity with a third party; upskirting and initiation/hazing type violence and rituals. Addressing inappropriate behaviour (even if it appears to be relatively innocuous) **can** be an important intervention that helps prevent problematic, abusive and/or violent behaviour in the future.

Sexual violence and sexual harassment between children in schools and colleges

Context

Sexual violence and sexual harassment can occur between two children of any age and sex. It can also occur through a group of children sexually assaulting or sexually harassing a single child or group of children.

Children who are victims of sexual violence and sexual harassment will likely find the experience stressful and distressing. This will, in all likelihood, adversely affect their educational attainment. Sexual violence and sexual harassment exist on a continuum and may overlap, they can occur online and offline (both physical and verbal) and are never acceptable.

It is essential that **all** victims are reassured that they are being taken seriously and that they will be supported and kept safe. A victim should never be given the impression that they are creating a problem by reporting sexual violence or sexual harassment. Nor should a victim ever be made to feel ashamed for making a report. Staff should be aware that some groups are potentially more at risk. Evidence shows girls, children with special educational needs and disabilities (SEND) and LGBT children are at greater risk. Staff should be aware of the importance of:

- challenging inappropriate behaviours.
- making clear that sexual violence and sexual harassment is not acceptable, will never be tolerated and is not an inevitable part of growing up.
- not tolerating or dismissing sexual violence or sexual harassment as “banter”, “part of growing up”, “just having a laugh” or “boys being boys”; and
- challenging physical behaviours (potentially criminal in nature), such as grabbing bottoms, breasts and genitalia, pulling down trousers, flicking bras and lifting up skirts. Dismissing or tolerating such behaviours risks normalising them.

What is sexual violence and sexual harassment?

Sexual violence

It is important that school and college staff are aware of sexual violence and the fact children can, and sometimes do, abuse their peers in this way. When referring to sexual violence we are referring to sexual violence offences under the Sexual Offences Act 2003 as described below:

Rape: A person (A) commits an offence of rape if: he intentionally penetrates the vagina, anus or mouth of another person (B) with his penis, B does not consent to the penetration and A does not reasonably believe that B consents.

Assault by Penetration: A person (A) commits an offence if: s/he intentionally penetrates the vagina or anus of another person (B) with a part of her/his body or anything else, the penetration is sexual, B does not consent to the penetration and A does not reasonably believe that B consents.

Sexual Assault: A person (A) commits an offence of sexual assault if: s/he intentionally touches another person (B), the touching is sexual, B does not consent to the touching and A does not reasonably believe that B consents.

Causing someone to engage in sexual activity without consent: A person (A) commits an offence if: s/he intentionally causes another person (B) to engage in an activity, the activity is sexual, B does not consent to engaging in the activity, and A does not reasonably believe that B consents. (This could include forcing someone to strip, touch themselves sexually, or to engage in sexual activity with a third party.)

What is consent? Consent is about having the freedom and capacity to choose. Consent to sexual activity may be given to one sort of sexual activity but not another, e.g. to vaginal but not anal sex or penetration with conditions, such as wearing a condom. Consent can be withdrawn at any time during sexual activity and each time activity occurs. Someone consents to vaginal, anal or oral penetration only if s/he agrees by choice to that penetration and has the freedom and capacity to make that choice.

- a child under the age of 13 can never consent to any sexual activity.
- the age of consent is 16.
- sexual intercourse without consent is rape.

Sexual harassment

When referring to sexual harassment we mean 'unwanted conduct of a sexual nature' that can occur online and offline. When we reference sexual harassment, we do so in the context of child on child sexual harassment. Sexual harassment is likely to: violate a child's dignity, and/or make them feel intimidated, degraded or humiliated and/or create a hostile, offensive or sexualised environment.

Whilst not intended to be an exhaustive list, sexual harassment can include:

- sexual comments, such as: telling sexual stories, making lewd comments, making sexual remarks about clothes and appearance and calling someone sexualised names.
- sexual "jokes" or taunting.
- physical behaviour, such as: deliberately brushing against someone, interfering with someone's clothes (schools and colleges should be considering when any of this crosses a line into sexual violence - it is important to talk to and consider the experience of the victim) and displaying pictures, photos or drawings of a sexual nature; and
- online sexual harassment. This may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence. It may include: consensual and /or non-consensual sharing of nudes/semi-nudes
- sharing of unwanted explicit content
- upskirting (is a criminal offence)
- sexualised online bullying.
- unwanted sexual comments and messages, including, on social media.
- sexual exploitation; coercion and threats.

Upskirting

The Voyeurism (Offences) Act, which is commonly known as the Upskirting Act, came into force on 12 April 2019. 'Upskirting' is where someone takes a picture under a person's clothing (not necessarily a skirt) without their permission and or knowledge, with the intention of viewing their genitals or buttocks (with or without underwear) to obtain sexual gratification, or cause the victim humiliation, distress or alarm. It is a criminal offence. Anyone of any gender, can be a victim.

The response to a report of sexual violence or sexual harassment

The initial response to a report from a child is important. It is essential that all victims are reassured that they are being taken seriously and that they will be supported and kept safe. A victim should never be given the impression that they are creating a

problem by reporting sexual violence or sexual harassment. Nor should a victim ever be made to feel ashamed for making a report.

If staff have a concern about a child or a child makes a report to them, they should follow the referral process as set out from paragraph 41 in Part one of this guidance. As is always the case, if staff are in any doubt as to what to do they should speak to the designated safeguarding lead (or a deputy).

Additional advice and support – see KCSE 2020 Annexe B: [Keeping children safe in education - GOV.UK](#)

Appendix 4

LEAP Eckington School: COVID-19 – School Closure Safeguarding section deals with specific advice and guidance around Coronavirus (COVID 19) safeguarding in schools and covers both school reopening and procedures for closures. (It is anticipated that this section will be updated in light of any new closures/government advice and at this point this appendix is simply a possible template)

Further guidance can be found at: ([ADD Government link here as appropriate if new guidance issued](#))

This is an addendum to our LEAP Safeguarding policy, which is still our fundamental guidance.

During this partial school closure:

A number of important safeguarding principles remain the same:

- with regard to safeguarding, the best interests of children must always continue to come first
- if anyone in a school or college has a safeguarding concern about any child they should continue to act immediately
- a DSL or deputy should be available
- it is essential that unsuitable people are not allowed to enter the children's workforce and/or gain access to children
- children should continue to be protected when they are online

1. Working with the Local Authority and school opening for critical worker / vulnerable children

The LA is responsible for social care. Social workers and the Virtual School continue to work with our most vulnerable

- students who are Looked After (LAC),
- have Child Protection Plans (CP)
- Child in Need Plans (CIN)
- students plus those who have an Education, Health and Care Plan (EHCP)

We will offer places to these students as well as those we view to be particularly vulnerable as outlined in DFE guidance and any others who have experienced family crisis or severe mental health issues over the past few weeks.

These children all have the opportunity to attend school along with the children of critical workers.

2. Attendance

During a lockdown lockdown or partial school closure: we will complete the daily Education Setting Status form via the DFE online portal as well as any LA required forms.

- **Attendance of vulnerable students:** school will continue to keep attendance records as directed by DFE and share data as required with both the DFE and LA. Social workers (and VS for LAC students) need to be notified when a child is absent from school to ensure appropriate follow up.
- All students in the above vulnerable categories are expected to attend school, where it is safe to do so (see DFE information about clinically vulnerable, risk assessing those with EHCP) – school will continue to work with parents and agencies to encourage attendance/inform on non-attendance.

- Where vulnerable students are not in school, then safe and well calls will continue as below.
- **Safeguarding – safe and well calls home by safeguarding, pastoral and attendance teams**

All the vulnerable category students as well as those who have an EHCP are on our safe and well calling list. In addition, those we deem “vulnerable” are also on the list. Over time, LoSDs and the safeguarding teams are adding students to this list, which is shared in OneDrive.

1. Calls will be **twice weekly** for most students on the list, **daily** for CP students and those we believe to be very vulnerable and **weekly** for others.
2. **Calling home** - use either SIMs or the safe and well calling contact spreadsheet in ONEDRIVE
3. If using your own phone- you MUST hide/withhold your number.
4. Explain that this is a safe and well call and ask how the child is, any concerns. If child is there – ask to speak to them to check how they are, how are they coping, do they have any concerns etc.
5. **Concerns:** If parents/child have concerns – we follow our usual procedures to reassure and signpost to support. Support information attached, also on website safeguarding page and student planners. Advise parents to contact social care if real concerns.
6. **If you have safeguarding concerns** – again follow our usual procedures, inform DSL/DSL team and Point 01629 533190 contact Derbyshire Starting Point where you believe a child is/maybe at risk of serious harm Derbyshire Starting Point Point 01629 533190. Sheffield MASH 0114 2734855
7. **Record keeping**
 - a) Log calls on CPOMs via the school system or directly at <https://eckington.cpoms.net>) using the **Closure safe & well call** category and noting date and time of call, who you spoke to and a summary of conversation & any actions. Alert safeguarding team and LoSD as usual to your CPOMs entry.
 - b) Safe and well calling spreadsheet: record daily contact made in the correct column

Outcome of call	Code to be used
Yes, spoke to parent	YP
Yes, spoke to child	YC
Yes, spoke to both parent and child	YPC
Voicemail	Voicemail
Unable to leave voicemail/contact	No contact
In school	In school

- c) Contact social worker/early help worker when contact made (& VS for LAC students) to help them co-ordinate their contact arrangements.

3. **What staff and volunteers should do if they have any concerns about a child**

It remains the case that if anyone in a school or college has a safeguarding concern about any child they should continue to **act immediately**.

School is open/partially open: If you are in school, then normal safeguarding procedures should be followed.

There will be a member of the safeguarding team* on site each day or a member of SLT - so they are on hand to deal with issues arising for both students in school and working from home.

School is closed/out of hours

All staff should react immediately if they have concerns about a child – logged on CPOMs and **safeguarding team and LoSD team alerted** (see page 4 staff planner for details about logging into CPOMs either directly <https://eckington.cpoms.net> or via school links).

Concerns about imminent danger/risk of serious harm: if you are unable to immediately contact a member of the safeguarding team, then contact the safeguarding hub yourself:

Derbyshire - 01629 533190

Sheffield – 0114 2734855

Please then record your actions on CPOMs.

In the event of school closure we will email/give students advice sheets about keeping safe, they will also be reminded to check their planners (pages 10-12). Information is also on the safeguarding page of the website

DSL team*- it is vital that we continue to safeguard our students and our DSL team is either in school on a rota, or working from home: Alison Burgess, Jim Taylor, Rebecca Price, Amanda Gregory, Katherine Needham.

On CPOMs - safeguarding team alerts go to the whole team. ALWAYS ensure that you include the safeguarding team in any CPOMs alerts as well as emails. The safeguarding email is alison.burgess@eck.leaptrust.co.uk

4. **Safer recruitment:** during this partial school closure we will respond to any new government advice, but use this plan as a basis of our process:

- Application process remains the same until the interview stage: virtual interviews replacing face to face interviews.
- It is important that all staff and volunteers are checked carefully as outlined in the LEAP safeguarding policy to ensure the requirements of Keeping Children safe in Education are implemented. However, the DFE have made the following temporary changes (March 2020 – we would update procedures in light of new guidance should schools be closed again) to the DBS standard and enhanced ID checking guidance:
 - ID documents to be viewed over video link
 - scanned images to be used in advance of the DBS check being submitted
 - the applicant will be required to present the original versions of these documents when they first attend their employment or volunteering role (we would await new government confirmation of this process and amend our procedure accordingly)

- Checking the right to work – (see latest Home Office guidance regarding checks) to see if they can be carried out over video calls, whether job applicants and existing workers can send scanned documents or a photo of documents for checks using email or a mobile app, rather than sending originals.
5. Should we move to a **school hub** situation for staff– then this section will be updated.
 6. Any **volunteers** would still be subject to the agreed LEAP Volunteers procedures.
 7. **Online safety – remote teaching and learning**

It is important that all staff who interact with children, including online, continue to look out for signs a child may be at risk and respond appropriately as outlined above.

In order to maintain proper safeguarding of students and staff, it is imperative that the following guidance is adhered to. Live lessons should follow our agreed protocols and only those with permission should be allowed to join live lessons.

The first duty of staff is to ensure the safety of our students. The provision of both live and video lessons must not compromise this.

Staff are expected to plan and provide online learning during closure; DFE guidance states that this should include both live and recorded lessons. As a broad principle during live lessons, **behave, and expect your students to behave, in this online space just as you and they would in school.** We have a duty to safeguard students when working online and all concerns should be reported as outlined above. The staff code of conduct and acceptable use policy are to be followed at all times.

1. **TEAMs** - should be the main learning platform for students and method for staff to communicate with students and set work.
2. **Email** - staff should only communicate with students via work email to a student's school email account. Staff PERSONAL accounts should NOT be used, nor should staff email a student's personal account.
3. **Asynchronous (anytime) video – recorded lessons**
 - a. There are advantages to recording video (or audio) rather than engaging in live video or audio sessions. You have a lot more control over the final presented form/content and can take your time to get things how you want them. Students can watch or listen to this content in their own time, and at their own pace - it's easy to wind back or fast forward if needed.
 - b. Such recordings must only be made and broadcast via school-based systems i.e. TEAMs
 - c. Key safeguarding principles need to be adhered to as described above when conducting a live lesson or recording a lesson. You need to be professional at all times: dressed appropriately, suitable background (not a bedroom; background not showing family photos; no background features to reveal home address or compromise family personal details / data; etc.)
 - d. Make sure that your LM is aware of the recording (they should check it prior to it being shared) which should be uploaded to a Sharepoint library for reference.

- e. Further guidance can be in the LEAP Remote Teaching and Safeguarding Guidance: https://leapmat-my.sharepoint.com/:w:/g/personal/mark_hardisty_leap-mat_org_uk/EbyF6ZV2EtJlJc5Ybu-539UB5s9-jsltbZTR3lgCp8uueQ?e=lfW0nx . There is also guidance and tips shared via the school home page.
- f. Be aware that students might still take screenshots, run audio recorders or run their own screen-recorders during these sessions, even if instructed not to. In a classroom context this invasion of privacy would be blatant and swiftly dealt with, but you are unlikely to notice if this happens online.

4. **Live lessons** -

Hosting a livestream means any situation where the school instigates, publishes and is responsible for streaming online content. This includes livestreaming lessons, assemblies and announcements.

- a. Prior to any session, we need to ensure that all parents have given permission. The consent form outlines expectations as described here: *Parental responsibility to ensure that NAME'S access to live lessons must be in an appropriate space in the home (not a bedroom; background not showing family photos; no background features to reveal home address or compromise family personal details / data; etc.). This is a precaution as student cameras are to be switched off as part of MS Teams settings*
Parents/carers understand that access to live lessons may be withdrawn if NAME does not comply with these conditions and if NAME in any way makes inappropriate use of lesson or video content.
Permissions are collected centrally, linked to SIMs and the MS Teams class groups for you.
- b. **BEFORE** you begin planning a live session, you must read the LEAP Remote Teaching and Safeguarding Guidance document: https://leapmat-my.sharepoint.com/:w:/g/personal/mark_hardisty_leap-mat_org_uk/EbyF6ZV2EtJlJc5Ybu-539UB5s9-jsltbZTR3lgCp8uueQ?e=lfW0nx as well as other guidance on the school homepage.
- c. The first duty of staff is to ensure the safety of students and as such 2 staff should be present or the lesson recorded and at least 2 students present.
Live streaming must not be 1-to-1.
There are a few exceptional circumstances, as agreed with the Principal (eg SEND bespoke work, KS5 tutoring) and where there is a **written agreement with parents** and possibly external agencies (eg consultant), outlining the circumstances of 1-to-1 tuition. In these circumstances, the agreed LEAP protocol must be followed.

If a live session (eg small group session) is planned and only one student attends, then the session can go ahead (as with all sessions, it is recorded) but the member of staff should notify their line manager at the end of the session to keep a record of this being a one to one session; the relevant HOY /SPL should also be notified.
- d. Live lessons/meetings **must be via Microsoft Teams.**
- e. Staff **MUST** be familiar with the privacy settings prior to using the streaming platform (see point b above)

- f. Staff must ensure that students are not able to communicate with each other after the staff have left the session – staff are the administrators and must ensure all students have left the session before they do (e.g. to **stop students rejoining a Teams call without the teacher there**, you must click **END MEETING** not the 'LEAVE' button).
 - g. Live sessions should be planned and kept to an appropriate length (ie usual lesson length as a maximum, but shorter input may be more effective with time for students to apply their learning to a task and then a possible plenary session). They should be in your usual lesson slot to avoid conflict with other subjects. BUT, staff need to consider whether all students in the class can access (eg some sharing resources) at that time and whether a pre-recorded session may be best, with a short follow up live session to check understanding etc.
 - h. Keep a record of the session (date/times/ register of who is involved, who left early and the time they left).
 - i. Recordings are saved to Microsoft Teams and to Microsoft Streams. Students must be informed that the session is being **recorded at the START of the meeting**
 - j. You need to be professional at all times: dressed appropriately, suitable background (not a bedroom; background not showing family photos; no background features to reveal home address or compromise family personal details / data; etc)
 - k. **Student cameras should be OFF**. Staff control mute/unmute to suit the teaching style/content. Students should be directed to use the “chat” facility and the “hands up” function. There is a student guide to support expectations.
 - k. Schools should ensure that staff using this technology to deliver lessons have access to their line manager and/or SLT colleagues in the event of a concern being raised.
 - l. Schools have the right, via staff, to withdraw access to live lessons if a student does not comply with the conditions of access and if a student in any way makes inappropriate use of lesson or video content. It maybe that a student’s online behaviour becomes disruptive, distracting or otherwise inappropriate and they are asked them to leave the shared space. If this happens, staff you follow school procedures to inform the LoSD and parents of this concern; appropriate records should be kept of this follow up action.
5. ICT support will assistance with uploading of content or access to live broadcasting, where required. They will also provide staff with guidance on recording, voice overs, etc, to help staff who wish to use this method of lesson delivery.
- Staff should remind students that-
Online safety is our number one priority. This live lesson is provided to help with your learning. If you have any concerns regarding online safety, report them to a family member, teacher or other adult.
6. **Mental health and well-being** – we are very conscious that these are unprecedented times and as such will affect children and adults in different ways. For students and staff, we have lost our usual support mechanisms in school and it may be a while before these are fully re-established. We have

signposted our students to various sources of advice and support – these were emailed to students, shown on social media and are on the website. We continue to use social media to send messages and advice to students and parents.

Before a year group returns, we will be asking families to update us on any changes regarding welfare, health and well-being, to help us to support students appropriately. We recognise that a period lockdown and a return to school and the routines of school-based learning, will be a significant challenge to some students.

Staff are encouraged to create social support groups online and we have put in place weekly check-ins via our line management pyramid to support colleagues. Weekly e briefings are also in place to support staff and keep them informed of developments. Senior leaders are available via the SLT email, ensuring staff always have access to support. As we return to wider school re-opening, we will communicate the planning and create opportunities for staff to ask questions and visit the site prior to returning to classes resuming on a wider scale.

7. **Peer on peer abuse** – given that students are operating online now, be mindful of any reports of online abuse. If these come to your attention – please report to LoSD and safeguarding team.

APPENDIX 5 INTERNET SETTINGS

DEFAULT SETTINGS

For purposes of filtering, LEAP MAT's baseline web filter identifies three groups of users:

- BYOD - All devices connecting via Wi-Fi that are unauthenticated
- STAFF - All Staff
- STUDENTS - All Students
- LAB - All Students in a Computing Lab Environment

SAFE SEARCHING

The majority of web search engines have the ability to filter out explicit content for all queries across images, videos and website. Whilst SafeSearches are not 100% accurate they are designed to help block explicit results, like pornography, from search queries.

BYOD	STUDENT	STAFF
ON	ON	ON

YOUTUBE

Similar to SafeSearch, YouTube offers its own safety feature to filter explicit and unsuitable content. It has two levels of filtering, STRICT and MODERATE. As with SafeSearch, YouTube filtering isn't 100% accurate and relies on an automated system that analyses the video's content, as well as the results of human moderators who apply an age restriction to videos.

BYOD	STUDENT	STAFF
OFF	STRICT	OFF

CATEGORY FILTERS

Internet searches are categorised by FortiGuard and allowed or blocked based upon industry standards and LEAP MAT's commitment to upholding stringent eSafeguarding and PREVENT duties.

Key

Category Descriptions & Contents

For more information on which sites are classified within these categories visit: <https://fortiguard.com/webfilter/categories>

Potentially Liable	BYOD / STUDENT/ LAB	STAFF
• Child Abuse	<input type="checkbox"/>	<input type="checkbox"/>
• Discrimination	<input type="checkbox"/>	<input type="checkbox"/>
• Drug Abuse	<input type="checkbox"/>	<input type="checkbox"/>
• Explicit Violence	<input type="checkbox"/>	<input type="checkbox"/>
• Extremist Groups	<input type="checkbox"/>	<input type="checkbox"/>
• Hacking	<input type="checkbox"/>	<input type="checkbox"/>
• Illegal or Unethical	<input type="checkbox"/>	<input type="checkbox"/>
• Plagiarism	<input type="checkbox"/>	<input type="checkbox"/>
• Proxy Avoidance	<input type="checkbox"/>	<input type="checkbox"/>

Adult/Mature	BYOD / STUDENT	STAFF
• Abortion	<input type="checkbox"/>	<input type="checkbox"/>
• Advocacy Organization	<input type="checkbox"/>	<input type="checkbox"/>
• Alcohol	<input type="checkbox"/>	<input type="checkbox"/>
• Alternative Beliefs	<input type="checkbox"/>	<input type="checkbox"/>
• Dating	<input type="checkbox"/>	<input type="checkbox"/>
• Gambling	<input type="checkbox"/>	<input type="checkbox"/>
• Lingerie and Swimsuit	<input type="checkbox"/>	<input type="checkbox"/>
• Marijuana	<input type="checkbox"/>	<input type="checkbox"/>
• Nudity and Risque	<input type="checkbox"/>	<input type="checkbox"/>
• Other Adult Materials	<input type="checkbox"/>	<input type="checkbox"/>
• Pornography	<input type="checkbox"/>	<input type="checkbox"/>
• Sex Education	<input type="checkbox"/>	<input type="checkbox"/>
• Sports Hunting and War Games	<input type="checkbox"/>	<input type="checkbox"/>
• Tobacco	<input type="checkbox"/>	<input type="checkbox"/>
• Weapons (Sales)	<input type="checkbox"/>	<input type="checkbox"/>

Bandwidth Consuming	BYOD / STUDENT	STAFF
• File Sharing and Storage	<input type="checkbox"/>	<input type="checkbox"/>
• Freeware and Software Downloads	<input type="checkbox"/>	<input type="checkbox"/>
• Internet Radio and TV	<input type="checkbox"/>	<input type="checkbox"/>
• Internet Telephony	<input type="checkbox"/>	<input type="checkbox"/>
• Peer-to-Peer File Sharing	<input type="checkbox"/>	<input type="checkbox"/>
• Streaming Media and Download	<input type="checkbox"/>	<input type="checkbox"/>

Security Risk	BYOD / STUDENT	STAFF
• Dynamic DNS	<input type="checkbox"/>	<input type="checkbox"/>
• Malicious Websites	<input type="checkbox"/>	<input type="checkbox"/>
• Newly Observed Domains	<input type="checkbox"/>	<input type="checkbox"/>
• Newly Registered Domains	<input type="checkbox"/>	<input type="checkbox"/>
• Phishing	<input type="checkbox"/>	<input type="checkbox"/>
• Spam URLs	<input type="checkbox"/>	<input type="checkbox"/>

General Interest – Personal	BYOD / STUDENT	STAFF
• Advertising	<input type="checkbox"/>	<input type="checkbox"/>
• Arts and Culture	<input type="checkbox"/>	<input type="checkbox"/>
• Auction	<input type="checkbox"/>	<input type="checkbox"/>
• Brokerage and Trading	<input type="checkbox"/>	<input type="checkbox"/>
• Child Education	<input type="checkbox"/>	<input type="checkbox"/>
• Content Servers	<input type="checkbox"/>	<input type="checkbox"/>
• Digital Postcards	<input type="checkbox"/>	<input type="checkbox"/>
• Domain Parking	<input type="checkbox"/>	<input type="checkbox"/>
• Dynamic Content	<input type="checkbox"/>	<input type="checkbox"/>
• Education	<input type="checkbox"/>	<input type="checkbox"/>
• Folklore	<input type="checkbox"/>	<input type="checkbox"/>
• Games	<input type="checkbox"/>	<input type="checkbox"/>
• Global Religion	<input type="checkbox"/>	<input type="checkbox"/>
• Health and Wellness	<input type="checkbox"/>	<input type="checkbox"/>

• Instant Messaging	<input type="checkbox"/>	<input type="checkbox"/>
• Job Search	<input type="checkbox"/>	<input type="checkbox"/>
• Meaningless Content	<input type="checkbox"/>	<input type="checkbox"/>
• Medicine	<input type="checkbox"/>	<input type="checkbox"/>
• News and Media	<input type="checkbox"/>	<input type="checkbox"/>
• Newsgroups and Message Boards	<input type="checkbox"/>	<input type="checkbox"/>
• Personal Privacy	<input type="checkbox"/>	<input type="checkbox"/>
• Personal Vehicle	<input type="checkbox"/>	<input type="checkbox"/>
• Personal Website and Blogs	<input type="checkbox"/>	<input type="checkbox"/>
• Political Organisations	<input type="checkbox"/>	<input type="checkbox"/>
• Real Estate	<input type="checkbox"/>	<input type="checkbox"/>
• Reference	<input type="checkbox"/>	<input type="checkbox"/>
• Restaurant and Dining	<input type="checkbox"/>	<input type="checkbox"/>
• Shopping	<input type="checkbox"/>	<input type="checkbox"/>
• Social Networking	<input type="checkbox"/>	<input type="checkbox"/>
• Society and Lifestyles	<input type="checkbox"/>	<input type="checkbox"/>
• Sports	<input type="checkbox"/>	<input type="checkbox"/>
• Travel	<input type="checkbox"/>	<input type="checkbox"/>
• Web Chat	<input type="checkbox"/>	<input type="checkbox"/>
• Web-based Email	<input type="checkbox"/>	<input type="checkbox"/>

General Interest - Business	BYOD / STUDENT	STAFF
• Armed Forces	<input type="checkbox"/>	<input type="checkbox"/>
• Business	<input type="checkbox"/>	<input type="checkbox"/>
• Charitable Organisations	<input type="checkbox"/>	<input type="checkbox"/>
• Finance and Banking	<input type="checkbox"/>	<input type="checkbox"/>
• General Organisations	<input type="checkbox"/>	<input type="checkbox"/>
• Government and Legal Organisations	<input type="checkbox"/>	<input type="checkbox"/>
• Information Technology	<input type="checkbox"/>	<input type="checkbox"/>
• Information and Computer Security	<input type="checkbox"/>	<input type="checkbox"/>
• Online Meeting	<input type="checkbox"/>	<input type="checkbox"/>
• Remote Access	<input type="checkbox"/>	<input type="checkbox"/>
• Search Engines and Portals	<input type="checkbox"/>	<input type="checkbox"/>
• Secure Websites	<input type="checkbox"/>	<input type="checkbox"/>
• Web Analytics	<input type="checkbox"/>	<input type="checkbox"/>
• Web Hosting	<input type="checkbox"/>	<input type="checkbox"/>
• Web-based Applications	<input type="checkbox"/>	<input type="checkbox"/>

Unrated	BYOD / STUDENT	STAFF
• Unrated	<input type="checkbox"/>	<input type="checkbox"/>

APPENDIX 6

STUDENT ACCEPTABLE USE POLICY (AUP)

By logging onto the network, you have accepted the school's acceptable use policy (AUP) for the remainder of the academic year. Misuse of IT facilities will result in these services being withdrawn.

Students should:

- Use the school's IT facilities appropriately as directed by the teacher for educational purposes only
- Use only the programs listed in the start menu as directed by the teacher
- Use only the programs identified by the teacher in the lesson
- Use only the websites identified by the teacher
- Print only when necessary and after consultation with the teacher

Note:

- All user activity is recorded including file creation, amending, execution, copying and deleting
- All user activity on the internet is recorded and filtered
- Certain file types cannot be saved onto the network
- There is a limit on user's network storage space. Regular checks are made on user storage areas
- Files which have inappropriate names or images which are deemed inappropriate will be deleted
- Limited print quotas will be allocated to all students

Misuse of IT facilities includes amongst other things:

- Using another person's account
- Use of proxy anonymizer sites and any technology which bypasses internet filtering and monitoring
- Pressing the keyboard and clicking the mouse of another student's computer without permission
- Pulling out/moving leads, switches and connections from any IT equipment
- Not using the internet for the purpose identified by the teacher
- Unnecessary and inappropriate use of printing facilities
- Changing the settings of any IT resource including computers, printers, projectors, cameras etc.
- Copying or running unauthorised programs such as games, scripts, spyware, malware, media players, file or network utilities, remote desktops etc.
- Running non-school programs, scripts or any other executables from removable media
- Damage or theft of IT equipment
- Any other usage which the school considers a threat to the security of students, information and/or resources

APPENDIX 7

STAFF ICT ACCEPTABLE USE POLICY (AUP)

You must adhere to LEAP MAT Data Protection and Privacy policies, eSafeguarding Policy and the following Acceptable Use Policy (AUP) when using IT services both in and out of school:

- Usernames, passwords and other logon credentials should be kept secure and not revealed to anyone else
- PCs should be logged out when not in use or locked whenever you are away from the device for a period of time
- You should ensure that any personal or sensitive data you use or access (SIMS, Assessment, SEN, Safeguarding, etc) is kept secure and used appropriately
- Ensure that when accessing personal or sensitive data that PC screens are not left unlocked in view of students, or that sensitive data is not broadcast via classroom projectors
- Do not allow an unauthorised person to access Trust ICT services using your credentials
- Any online activity should not harass, harm, offend or insult others
- You must not search for, download, upload, or distribute content that is illegal, or that could be considered offensive by another user. If you accidentally encounter such material you should report this immediately to the IT Support team
- You should not download or install any software or hardware without permission. If you have responsibility for purchasing software, you should be confident that it is adequately licenced and appropriate for educational use
- USB/external storage devices should not be used unless explicit permission is granted by the Principal. Staff are encouraged to use OneDrive to securely work on documents between home and school. **No personal data whatsoever should ever be held on a USB/external hard drive**
- Any sensitive data that needs to be taken off-site should be held on OneDrive, accessed via www.office.com and not synchronised to any personal device. OneDrive folders synchronised to Trust managed devices is acceptable, where those devices are encrypted with BitLocker or equivalent technologies. If data needs to be taken off-site and OneDrive is not suitable, then data can be held and transported on an encrypted USB drive as authorised by the Principal
- Any electronic communication should be related to Trust business only and should be through Trust e-mail addresses or other appropriately sanctioned communication systems (such as SIMS InTouch)
- Any digital mixed media content of students and staff should be for Trust purposes only. They should be recorded on school equipment and stored securely on LEAP MAT's ICT infrastructure
- You must never provide your personal details, or the personal details of others to students or parents, or publicly on the internet. For using social media, see the relevant policy
- You should promote and support the school eSafeguarding Policy and Data Protection and Privacy Policies, and promote and model safe and responsible behaviour in students when using ICT to support teaching and learning
- Any ICT equipment used or borrowed from LEAP MAT should be used in accordance with this AUP at all times. If taken off-site, the equipment should be returned annually for an electrical safety check and to ensure compliance with secure IT policies. On leaving the employ of LEAP MAT, the equipment should be returned in good order to the IT Team prior to leaving
- Particular care should be taken to ensure that any sensitive information shared or emailed to other colleagues or external agencies is kept secure in transfer and that you are certain of the correct recipient. Any data that potentially has

- been transmitted insecurely, or to an unauthorised party should immediately be reported to the IT Support team
- You must report all suspected or potential IT security, eSafeguarding or data breaches to the IT Support team and the DPO

Live Lesson Code of Conduct

This Code of Conduct document must be read in conjunction with The Trust's IT Acceptable Use and Safeguarding Policy.

Parents and carers must agree to these expectations of their children before they can participate in live lessons.

CODE OF CONDUCT

Before attending a live lesson, students must ensure:

- They are located in an appropriate space for video broadcasting – not a bedroom, an open-plan, shared space where possible, without family photos or any other background feature that could reveal or compromise family or personal details. Teams backgrounds can be used to hide the home.
- They are dressed appropriately.

When attending, students must:

- Attend promptly as per the given timetable. The teacher will issue a “meet now” or start the lesson using another mechanism depending on Academy just before the meeting time.
- Give notice in advance, to subject teachers if they cannot attend and state the reason. Then if possible, watch the lesson at a later time.
- Mute their microphone and switch off their camera until instructed to do otherwise. Students must maintain the high standards of behaviour expected by The Trust by:
 - Only taking part in the session at the appropriate time and in the manner expected, given that all actions including audio, video and chat are monitored and recorded.
 - Only take part in lessons that they are invited to.
 - Not engaging in any spoken or written, or other language or behaviour that could be deemed inappropriate or offensive either visually, verbally or through the discussion functions.
 - Not filming or photographing any other student or teacher taking part in the live lesson, during or from the session video that is made available afterwards.
 - Not photographing any shared screens/work during the session. A recording will be made available afterwards if anything was missed.
 - Requesting clarification, and by asking questions as directed by the lesson teacher and by using the “Hands Up” function in Teams to await their turn to respond or using the Team Chat function so the teacher can see your question.
 - Being respectful to all of those involved in the lesson.

DISCIPLINARY PROCEDURE

If a student is not behaving in accordance with the expectations above, then depending on the severity of the incident they will be warned by the class teacher, or if further incidents occur they will be removed from the lesson and the matter escalated. Teachers can remove students from the lesson at the first incident if they deem it to be serious enough. Students cannot then return to the lesson.

With escalations, further sanctions may occur, including removal from live lessons indefinitely and as such breaches of this code of conduct be reported to a Pastoral Leader or Senior Leader.