Grove Learning Trust

Online Safety Policy

Ratified by Standards & Performance Committee

Spring 2025

Contents

Introduction 2
Scope of the Online Safety Policy 3
Responsibilities 3
Acceptable Use Agreements 10
Reporting and responding 14
Online Safety Incident Flowchart 17
Online Safety Education Programme 18
Filtering & Monitoring 19
Filtering 20
Monitoring 20
Mobile technologies 21
Social media 22
Appendices List 25
A1: Learner Acceptable Use Agreement – for EYFS / KS1 26
A2: Learner Acceptable Use Agreement – for KS2 27
A3: Staff and Volunteer Acceptable Use Agreement 29
A4: Acceptable Use Agreement for Community Users 32
A5: Online Safety Group - Terms of Reference 34
A6: Responding to incidents of misuse – flow chart 36
A7: Record of reviewing devices/internet sites (responding to incidents of misuse) 37
A8: Reporting Log 38
A9: Training Needs Audit Log 39
Legislation 40
Links to other Organisations 46
    Tools for Schools / other organisations 46
    Bullying/Online-bullying/Sexting/Sexual Harassment 46
    Infrastructure/Technical Support/Cyber-security 47
Version Control 49
Review 49

Introduction

The DfE Keeping Children Safe in Education statutory guidance requires Local Authorities, Multi Academy Trusts, and schools in England to ensure learners are safe from harm:

"It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate"

"Governing bodies and proprietors should ensure online safety is a running and interrelated theme whilst devising and implementing their whole school or college approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement"

The DfE Keeping Children Safe in Education guidance also recommends:

Reviewing online safety … Technology, and risks and harms related to it, evolve, and change rapidly. Schools and colleges should consider carrying out an annual review of their approach to online safety, supported by an annual risk assessment that considers and reflects the risks their children face. Free online safety self-review tools for schools are available through the grid for learning networks.

The DfE Keeping Children Safe in Education guidance suggests that:

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism. This now includes **misinformation, disinformation and conspiracy theories**, which can distort understanding and influence harmful behaviours.

contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and

commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Schools in England have their online safety practices evaluated through Ofsted inspectors, and the Counter Terrorism and Securities Act 2015 requires schools to ensure that children and young people are safe from terrorist and extremist material on the internet.

Scope of the Online Safety Policy

This online safety policy outlines the commitment of Grove Learning Trust to safeguard members of our school community online in accordance with statutory guidance and best practice. Schools are aware of the legislative framework under which this online safety policy has been produced as outlined in the attached 'Legislation' appendix.

This online safety policy applies to all members of the school community (including staff, learners, trustees, academy committee governors, volunteers, parents and carers, visitors and community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site.

This online safety policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication.
- allocates responsibilities for the delivery of the policy.
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours.
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world.
- describes how the school will help prepare learners to be safe and responsible users of online technologies.
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms.
- is supplemented by a series of related acceptable use agreements.
- is made available to staff at induction and through normal communication channels.
- is published on the school website.

Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

Headteacher and Senior Leaders

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.

- The headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

- The headteacher is responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.

- The headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.

- The headteacher will receive or access regular monitoring reports in relation to online safety and filtering.

- The headteacher will work with the link academy committee governor, the designated safeguarding lead and IT service providers in all aspects of filtering and monitoring.

Trustees and Academy Committee Governors

The DfE guidance "Keeping Children Safe in Education" states:

*"Governing bodies and proprietors (this is the **trustees** in GLT) should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children's welfare …. this includes … online safety"*

"Governing bodies and proprietors should ensure an appropriate senior member of staff, from the school or college leadership team, is appointed to the role of designated safeguarding lead. The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place)"

Trustees are responsible for the approval of the online safety policy and **academy committee governors** are responsible for reviewing the effective implementation of the policy through the termly headteachers report and link roles.

A member of the **academy committee** in each school will take on the role of online safety governor. This can be the same person that is the link for safeguarding. The link role will include meetings with the DSL and / or the online safety lead so the academy committee is assured that:

- reports of online safety incidents are recorded and actioned in a timely manner
- online safety education provision and staff training is taking place regularly
- filtering and monitoring provision is in place and regularly reviewed by the DSL or online safety lead - in-line with the DfE Filtering and Monitoring Standards

The strategic safeguarding lead for the trust will report to **trustees** on the effective implementation of this policy through the safeguarding dashboard.

Designated Safety Lead (DSL)

Keeping Children Safe in Education states that:

"The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). This should be explicit in the role holder's job description."

They (the DSL) "are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college"

They (the DSL) "can recognise the additional risks that children with special educational needs and disabilities (SEND) face online, for example, from bullying, grooming and radicalisation and are confident they have the capability to support children with SEND to stay safe online"

While the responsibility for online safety is held by the DSL and cannot be delegated, the school may choose to appoint an online safety lead or other relevant persons to work in support of the DSL in carrying out these responsibilities. Each Grove Learning Trust school will allocate roles from the list below to reflect the individual structure in each setting.

The DSL will:

- hold the lead responsibility for online safety, within their safeguarding role.
- receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online.
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out.
- attend relevant governing body meetings to answer questions relating to online safety.
- report on online safety regularly to the headteacher and wider senior leadership team.
- be responsible for receiving reports of online safety incidents and handling them and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety) .

The following list is the responsibility of the DSL, unless there is a separate online safety lead. Where there is an online safety lead, they will:

- work closely on a day-to-day basis with the DSL.

- receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments.
- have a leading role in establishing and reviewing the school online safety procedures.
- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond.
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated.
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents.
- provide, or identify sources of, training and advice for staff, academy committee governors, parents, carers and learners.
- liaise with technical staff, pastoral staff and support staff (as relevant).
- receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education:
    - content
    - contact
    - conduct
    - commerce

Curriculum Leads

Curriculum leads will work with the DSL and online safety lead (where there is one) to develop a planned and coordinated online safety education programme.

This will be provided through:

- the computing and IT curriculum
- PHSE and SRE programmes
- cross-curricular curriculum opportunities
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. ***Safer Internet Day*** and ***Anti-bullying week.***

Teaching and Support Staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters and trends and of the current school online safety policy and practices.
- they understand that online safety is a core part of safeguarding.
- they have read, understood, and signed the staff acceptable use agreement (AUA).
- they immediately report any suspected misuse or problem for investigation and action, in line with the school safeguarding procedures.
- all digital communications with learners and parents / carers are on a professional level and only carried out using official school systems.
- online safety issues are embedded in all aspects of the curriculum and other activities.
- ensure learners understand and follow the online safety policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities and implement current policies regarding these devices.
- in lessons where internet use is pre-planned learners are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc.
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

IT Provider

The DfE Filtering and Monitoring Standards says:

"Senior leaders should work closely with governors or proprietors, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring. Your IT service provider may be a staff technician or an external service provider."

"Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL should work closely together with IT service providers to meet the needs of your setting. You may need to ask filtering or monitoring providers for system specific training and support."

"The IT service provider should have technical responsibility for:

- *maintaining filtering and monitoring systems*
- *providing filtering and monitoring reports*
- *completing actions following concerns or checks to systems"*

"The IT service provider should work with the senior leadership team and DSL to:

- *procure systems*
- *identify risk*
- *carry out reviews*
- *carry out checks"*

"We are aware that there may not be full-time staff for each of these roles and responsibility may lie as part of a wider role within the school, college, or trust. However, it must be clear who is responsible, and it must be possible to make prompt changes to your provision."

It is the responsibility of the headteacher to ensure that the external IT provider carries out all the online safety measures that the school's obligations and responsibilities require. It is also important that the provider follows and implements school online safety policy and procedures.

The IT Provider is responsible for ensuring that:

- they are aware of and follow the school online safety policy to carry out their work effectively in line with school policy.
- the school technical infrastructure is secure and is not open to misuse or malicious attack.
- the school meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges.
- there is clear, safe, and managed control of user access to networks and devices.
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported for investigation and action.
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- monitoring systems are implemented and regularly checked.

Learners

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and online safety policy.

- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

- should know what to do if they or someone they know feels vulnerable when using online technology.

- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school.

Parents and Carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

The school will take every opportunity to help parents and carers understand these issues through:

- publishing the school online safety policy on the school website.
- providing them with a copy of the learners' acceptable use agreement.
- publish information about appropriate use of social media.
- seeking their permissions concerning digital images, cloud services etc.
- parents' / carers' evenings, newsletters, website, social media and information about national & local online safety campaigns and resources.

Parents and carers will be encouraged to support the school in:

- reinforcing the online safety messages provided to learners in school.
- the safe and responsible use of their children's personal devices in the school (where this is allowed).

Community Users

Community users who access school systems, websites and social media & learning platforms as part of the wider school provision, will be expected to sign a community user AUA before being provided with access to school systems. The community user's acceptable use agreement is in the appendices section.

The school encourages the engagement of agencies / members of the community who can provide valuable contributions to the online safety provision and actively seeks to share its knowledge and good practice with other schools and the community.

Online Safety Group

Grove Learning Trust recognises the collective responsibility to developing and implementing the online safety policy. An online safety group has therefore been established to provide wide representation from the trust community, with responsibility for issues regarding online safety and monitoring the online safety policy including the impact of initiatives. This group is led by the trust's strategic safeguarding lead.

The online safety group has the following members:

- designated safeguarding leads
- online safety leads
- academy committee online safety governor
- technical staff
- teacher and support staff representative
- school business managers

Members of the online safety group meet three times per academic year to:

- update, review and monitor the online safety policy documents.
- update, review and monitor the school filtering policy and its implementation.
- review samples of network, filtering, monitoring, incident logs.
- consulting stakeholders – including staff, parents, carers and learners about the online safety provision across Grove Learning Trust.
- monitor improvement actions identified through use of online safety self-review tools or from annual safeguarding audits where the recommendation relates to online safety.

Acceptable Use Agreements

Grove Learning Trust has defined what it regards as acceptable / unacceptable use and this is shown in the tables below.

Acceptable use agreements outline our trust expectations on the responsible use of technology by its users. They are signed by their staff as part of their conditions of employment. They are regularly promoted with parents / carers and learners, so they are understood and followed. The Grove Learning Trust acceptable use agreements are available in the appendices.

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that	**Any illegal activity for example:** • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
contain or relate to:	• Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering A useful reference document for further guidance about dealing with self-generated images/sexting is included here – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access. • Gaining unauthorised access to school networks, data and files, through the use of computers/devices. • Creating or propagating computer viruses or other harmful files. • Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords). • Disable / Impair / Disrupt network functionality through the use of computers / devices. • Using penetration testing equipment (without relevant permission).					X
Users shall not undertake activities that are not illegal but are classed as unacceptable in trust and school policies:	Accessing inappropriate material / activities online in a school setting including pornography, gambling, drugs.				X	
	Promotion of any kind of discrimination.				X	
	Using school systems to run a private business.				X	
	Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by the school				X	
	Infringing copyright.				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet).			X	X	

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute.				X	

User actions	**Staff and other adults**				**Learners**			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission & supervision
Online gaming								
Online shopping/commerce								
File sharing								
Accessing personal social media accounts								
Accessing work / school related social media accounts								
Entertainment streaming e.g. Netflix, Disney+, Prime								

Use of video broadcasting for planned learning opportunities , e.g. YouTube								
Mobile phones may be brought to school								
Use of mobile phones during the school day								
Taking photos or record video on personal mobile phones/cameras								
Taking photos or record video on work mobile phones/cameras								
Use of other personal devices, e.g. tablets, gaming devices								
Use of personal e-mail in school, or on school network/wi-fi								
Use of school e-mail for personal e-mails								

When using communication technologies, Grove Learning Trust considers the following as good practice:

- when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school.
- any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. Personal e-mail addresses, text messaging or social media must not be used for these communications.
- staff are expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community.

- users must immediately report to the headteacher the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- professional conduct must be followed when posting information online e.g., school website and social media. Only school e-mail addresses should be used to identify members of staff and learners.

Reporting and responding

The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for schools to understand that reporting systems do not always respond to the needs of learners. While the report looks specifically at harmful sexual behaviours, schools may wish to address these issues more generally in reviewing their reporting systems. The Ofsted review suggested:

"School and college leaders should create a culture where sexual harassment and online sexual abuse are not tolerated, and where they identify issues and intervene early to better protect children and young people. ..In order to do this, they should assume that sexual harassment and online sexual abuse are happening in their setting, even when there are no specific reports, and put in place a whole-school approach to address them. This should include:

- *routine record-keeping and analysis of sexual harassment and sexual violence, including online, to identify patterns and intervene early to prevent abuse"*

Grove Learning Trust will take all reasonable precautions to ensure online safety for all trust users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

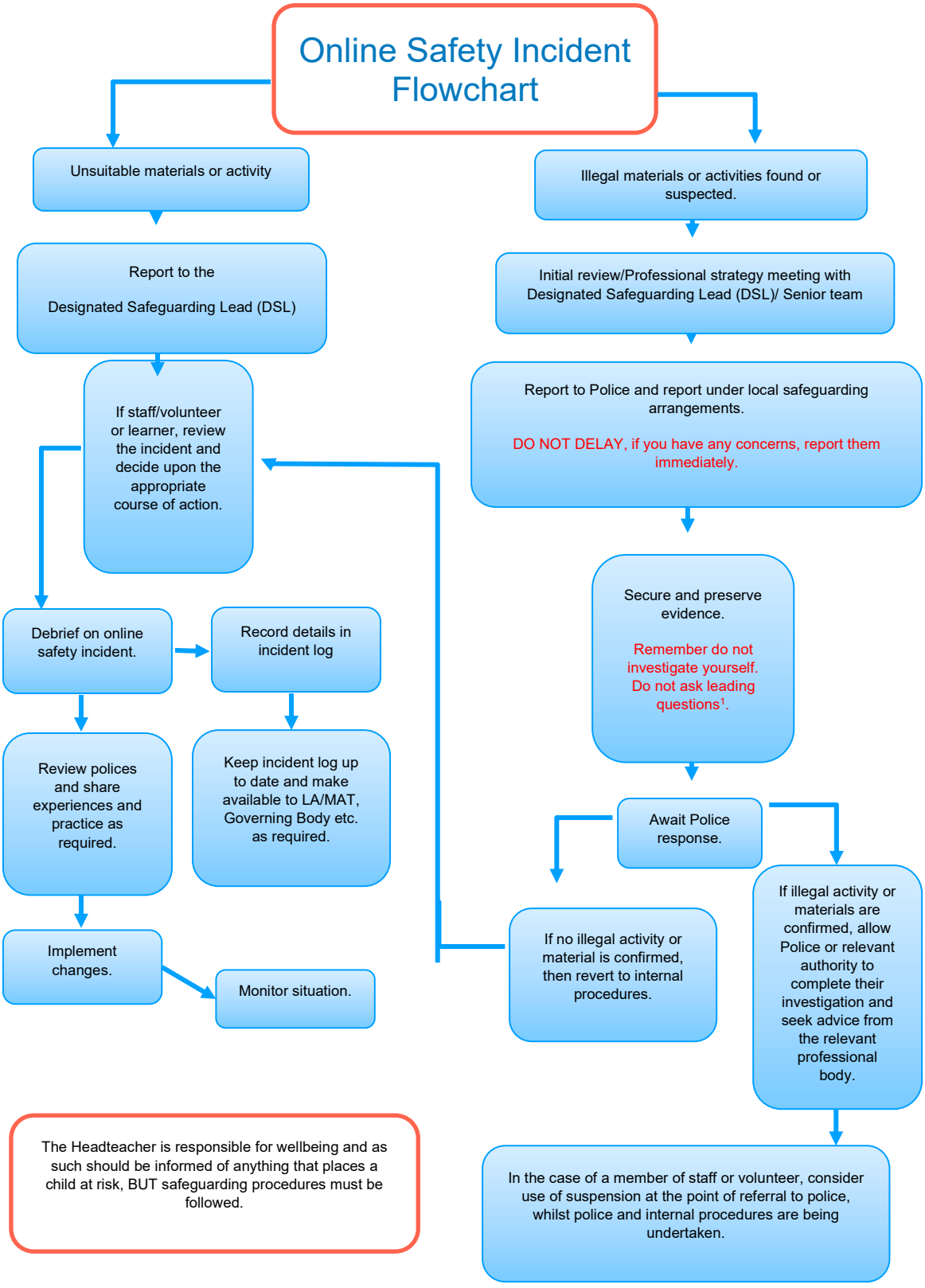
- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- all members of the school community will be made aware of the need to report online safety issues/incidents.
- reports will be dealt with as soon as is practically possible once they are received.
- the Designated Safeguarding Lead, online safety lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm (see flowchart and user actions chart in the appendix), the incident must be escalated through the agreed school safeguarding procedures, this may include
    - Non-consensual images
    - Self-generated images
    - Terrorism/extremism
    - Hate crime/ Abuse

    - Fraud and extortion
    - Harassment/stalking
    - Child Sexual Abuse Material (CSAM)
    - Child Sexual Exploitation Grooming
    - Extreme Pornography
    - Sale of illegal materials/substances
    - Cyber or hacking offences under the Computer Misuse Act
    - Copyright theft or piracy

- any concern about staff misuse will be reported to the headteacher, unless the concern involves the headteacher, in which case the complaint is referred to the trust's strategic safeguarding lead.
- where there is **no suspected illegal activity**, devices may be checked using the following procedures:
    1. two senior members of staff will be involved to protect individuals if accusations are subsequently reported.
    2. conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected).
    3. ensure that the sites and content visited are closely monitored and recorded (to provide further protection).
    4. record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots for investigation. These may be printed, signed, and attached to the form.
    5. once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
        - internal response or discipline procedures
        - involvement by local authority designated officer (LADO) / trust strategic safeguarding lead
        - police involvement and/or action
- incidents must be logged.
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (where appropriate to do so).
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
    1. the online safety group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with
    2. staff, through regular briefings

3. learners, through assemblies/lessons
4. parents/carers, through newsletters, school social media, website
5. trustees and academy committee governors, through regular safeguarding updates
6. local authority safeguarding agencies and external agencies, as relevant (The Ofsted Review into Sexual Abuse in Schools and Colleges suggested "working closely with Local Safeguarding Partnerships in the area where the school or college is located so they are aware of the range of support available to children and young people who are victims or who perpetrate harmful sexual behaviour")

The school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.


Online Safety Incident Flowchart
Unsuitable materials or activity
Illegal materials or activities found or suspected.
Report to the Designated Safeguarding Lead (DSL)
Initial review/Professional strategy meeting with Designated Safeguarding Lead (DSL)/ Senior team
If staff/volunteer or learner, review the incident and decide upon the appropriate course of action.
Report to Police and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Debrief on online safety incident.
Record details in incident log
Secure and preserve evidence.
Remember do not investigate yourself. Do not ask leading questions[1].
Review polices and share experiences and practice as required.
Keep incident log up to date and make available to LA/MAT, Governing Body etc. as required.
Await Police response.
Implement changes.
Monitor situation.
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body.
The Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.
In the case of a member of staff or volunteer, consider use of suspension at the point of referral to police, whilst police and internal procedures are being undertaken.

Online Safety Education Programme

While regulation and technical solutions are particularly important, their use must be balanced by educating learners to take a responsible approach. The education of learners in online safety is therefore an essential part of the school's online safety provision. Learners need the help and support of the school to recognise and avoid online safety risks and develop their resilience.

The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for:

"a carefully sequenced RSHE curriculum, based on the Department for Education's (DfE's) statutory guidance, that specifically includes sexual harassment and sexual violence, including online. This should include time for open discussion of topics that children and young people tell us they find particularly difficult, such as consent and the sending of 'nudes'.."

Keeping Children Safe in Education states:

"*Governing bodies and proprietors should ensure online safety is a running and interrelated theme whilst devising and implementing their whole school or college approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum …*"

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum for all year groups matched against a nationally agreed framework and regularly taught in a variety of contexts.
- Lessons are matched to need; are age-related and build on prior learning.
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes.
- Learner need and progress are addressed through effective planning and assessment.
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Literacy etc.
- The planned curriculum incorporates / makes use of relevant national initiatives and opportunities e.g. *Safer Internet Day* and *Anti-bullying week*
- The programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- Vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse and SEND.

- learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school. Acceptable use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990.
- In lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, learners may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

Filtering & Monitoring

The DfE guidance (for England) on filtering and monitoring in 'Keeping Children Safe in Education' states:

"It is essential that governing bodies and proprietors ensure that appropriate filtering and monitoring systems are in place ...governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the … risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified…

The appropriateness of any filtering and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty. To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards…"

The school filtering and monitoring provision is agreed by senior trust and school leaders and regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT service provider has technical responsibility.

The filtering and monitoring provision is reviewed (at least annually) by senior leaders and the Designated Safeguarding Lead with the involvement of the IT Service Provider.

Checks on the filtering and monitoring system are carried out by the IT service provider with the involvement of senior leaders and the Designated Safeguarding Lead, in particular when a safeguarding risk is identified, there is a change in working practice, e.g. remote access or new technology is introduced.

Filtering

The school manages access to content across its systems for all users and on all devices using the schools internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre *Appropriate filtering*.

Illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated.

There are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective.

There is a clear process in place to deal with, and log, requests/approvals for filtering changes (see Appendix for more details).

Filtering logs are regularly reviewed and the Designated Safeguarding Lead is alerted to breaches of the filtering policy, which are then acted upon.

If necessary, the school will seek advice from, and report issues to external partners and agencies.

Monitoring

The school has the following monitoring systems in place to protect the school, systems and users:

- The external IT support team monitors all network use across all devices and services.
- Reports of inappropriate activity are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead.
- All users are aware that the network (and devices) are monitored.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.

The school follows the UK Safer Internet Centre *Appropriate Monitoring* guidance and protects users and school systems through the use of the appropriate blend of strategies. These include:

- physical monitoring (adult supervision in the classroom)
- internet use logged and monitored / reviewed
- filtering logs analysed and breaches reported to the DSL
- use of a third-party assisted monitoring service

Mobile technologies

The DfE guidance "Keeping Children Safe in Education" states:

> *"The school or college should have a clear policy on the use of mobile and smart technology. Amongst other things this will reflect the fact many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school or college, sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content. Schools and colleges should carefully consider how this is managed on their premises and reflect this in their mobile and smart technology policy and their child protection policy."*

Mobile technology devices may be school owned/provided or personally owned and might include smartphone, tablet, wearable devices, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school learning platform and other cloud-based services such as e-mail and data storage.

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's online safety education programme.

The school acceptable use agreements for staff and learners outline the expectations around the use of mobile technologies.

The school allows:

	School devices			Personal devices		
	School owned for individual use	School owned for multiple users	Authorised device[1]	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	No	No	Yes
Full network access	Yes	Yes	Yes	No	No	No
Internet only	No	No	No	No	No	Yes

Social media

With widespread use of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of learners, the school and the individual when publishing any material online.

Expectations for teachers' professional conduct are set out in the DfE Teachers Standards but all adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

All schools and local authorities have a duty of care to provide a safe learning environment for learners and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, bully online, discriminate on the grounds of sex, race, or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:

- ensuring that personal information is not published.
- education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues.
- clear reporting guidance, including responsibilities, procedures, and sanctions.

[1] Authorised device – purchased by the learner/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

- risk assessments, where appropriate.
- guidance for learners, parents/carers.

School staff should ensure that:

- No reference should be made in social media to learners, parents/carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- They act as positive role models in their use of social media.

When official school social media accounts are established, there should be:

- A process for approval by senior leaders.
- Clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff.
- Systems for reporting and dealing with abuse and misuse.
- Understanding of how incidents may be dealt with under school disciplinary procedures.

Personal use

- Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
- The school permits reasonable and appropriate access to personal social media sites during school hours.

Monitoring of public social media

- As part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school.
- When parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

School use of social media for professional purposes will be checked regularly by a senior leader and online safety lead (where one is in post) to ensure compliance with the social media, data protection, communications, digital image and video procedures. In the event of any social media issues that the school is unable to resolve, support may be sought from external partners.

Appendices List

A1 - Learner Acceptable Use Agreement – for EYFS / KS1
A2 - Learner Acceptable Use Agreement – for KS2

A3 - Staff (and Volunteer) Acceptable Use Agreement

A4 - Community Users Acceptable Use Agreement

A5 – Online Safety Group Terms of Reference
A6 - Responding to incidents of misuse – flow chart
A7 - Record of reviewing devices/internet sites (responding to incidents of misuse)
A8 - Reporting Log

A9 - Training Needs Audit Log

Legislation

Links to other organisations and resources

A1: Learner Acceptable Use Agreement – for EYFS / KS1

This is how we stay safe when we use computers:

- I will ask a teacher or trusted adult if I want to use the computers, iPad or school devices.
- I will only use activities that a teacher or trusted adult has told or allowed me to use.
- I will take care of computers, iPad and other equipment.
- I will ask for help from a teacher or trusted adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or trusted adult if I see something that upsets me on the screen.
- I know that if I break the rules, I might not be allowed to use a computers, iPad or school device.

A2: Learner Acceptable Use Agreement – for KS2

Introduction

Digital technologies have become integral to the lives of children and young people, both within and outside schools. These technologies are powerful tools, which open-up new opportunities for everyone. They can stimulate discussion, encourage creativity, and stimulate awareness of context to promote effective learning. Learners should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended:

- to ensure that learners will have good access to devices and online content, be responsible users and stay safe while using digital technologies for educational, personal and recreational use
- to help learners understand good online behaviours that they can use in school, but also outside school
- to protect school devices and networks from accidental or deliberate misuse that could put the security of the systems and users at risk.

Acceptable Use Agreement

When I use devices I must behave responsibly to help keep me and other users safe online and to look after the devices.

For my own personal safety:

- I understand that what I do online will be supervised and monitored and that I may not be allowed to use devices in school unless I follow these rules and use them responsibly.
- I will only visit internet sites that adults have told me are safe to visit.
- I will keep my username and password safe and secure and not share it with anyone else.
- I will be aware of "stranger danger" when I am online.
- I will not share personal information about myself or others when online.
- If I arrange to meet people off-line that I have communicated with online, I will do so in a public place and take a trusted adult with me.
- I will immediately tell an adult if I see anything that makes me feel uncomfortable when I see it online.

I will look after the devices I use, so that the school and everyone there can be safe:

- I will handle all the devices carefully and only use them if I have permission.
- I will not try to alter the settings on any devices or try to install any software or programmes.
- I will tell an adult if a device is damaged or if anything else goes wrong.
- I will only use the devices to do things that I am allowed to do.

I will think about how my behaviour online might affect other people:

- When online, I will act as I expect others to act toward me.
- I will not copy anyone else's work or files without their permission.
- I will be polite and responsible when I communicate with others, and I appreciate that others may have different opinions to me.
- I will not take or share images of anyone without their permission.

I know that there are other rules that I need to follow:

- I will only use my own personal devices (mobile phones/USB devices etc.) in the school if I have permission. If I am allowed, I still have to follow all the other school rules if I use them.
- I will not use social media sites during the school day or on school devices.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I should have permission if I use the original work of others in my own work.

I understand that I am responsible for my actions, both in and out of school:

- I know that I am expected to follow these rules in school and that I should behave in the same way when out of school as well.
- I understand that if I do not follow these rules, I may be subject to disciplinary action. This could include loss of access to the school network/internet, parents/carers contacted and in the event of illegal activities involvement of the police.

A3: Staff and Volunteer Acceptable Use Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that learners receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.

- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured (unless for a specific purpose and permission from the individual has been gained).
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless permission has been given.

- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the online systems in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this acceptable use policy applies not only to my work and use of school's digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to the Local Authority Designated Officer for safeguarding and in the event of illegal activities, the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name: .....

Signed: .....

Date: .....

A4: Acceptable Use Agreement for Community Users

This acceptable use agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices.
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential harm in their use of these systems and devices.

Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school:

- I understand that my use of school systems and devices will be monitored.
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist and extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report to the headteacher or designated safeguarding lead any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and/or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured (unless permission has been given for the specific purpose by the individual).
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the headteacher.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, whatever the cause.

- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this acceptable use agreement, the school has the right to remove my access to school systems/devices and might terminate my use of the school facilities.

I have read and understand the above and agree to use the school systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name: .....

Signed: .....

Date: .....

A5: Online Safety Group - Terms of Reference

1. Purpose

To provide a consultative group that has wide representation from the Grove Learning Trust community, with responsibility for issues regarding online safety and the monitoring the online safety policy including the impact of initiatives

2. Membership

2.1. The online safety group will seek to include representation from all stakeholders.

The composition of the group will include:

- designated safeguarding leads
- online safety leads
- academy committee online safety governor
- technical staff
- teacher and support staff representative
- school business managers

2.2. Other people may be invited to attend the meetings at the request of the trusts strategic safeguarding lead, on behalf of the group, to provide advice and assistance where necessary.

2.3. Group members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.

2.4. Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature.

2.5. When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities.

3. Lead Person

The Grove Learning Trust strategic safeguarding lead will be the lead person for the group. Their responsibilities include:

- Scheduling meetings and notifying members
- Inviting other people to attend meetings when required
- Guiding the meeting according to the agenda and time available
- Ensuring all discussion items end with a decision, action or definite outcome
- Making sure that notes are taken at the meetings and that these, with any action points, are distributed as necessary

4. Duration and Frequency of Meetings

Meetings shall be held three times per academic year for a maximum of 1 hour per meeting.

5. Functions

The key functions of the online safety group are:

- update, review and monitor the online safety policy documents.
- update, review and monitor the school filtering policy and its implementation.
- review samples of network, filtering, monitoring, incident logs.
- consulting stakeholders – including staff, parents, carers and learners about the online safety provision across Grove Learning Trust.
- monitor improvement actions identified through use of online safety self-review tools or from annual safeguarding audits where the recommendation relates to online safety.

6. Amendments

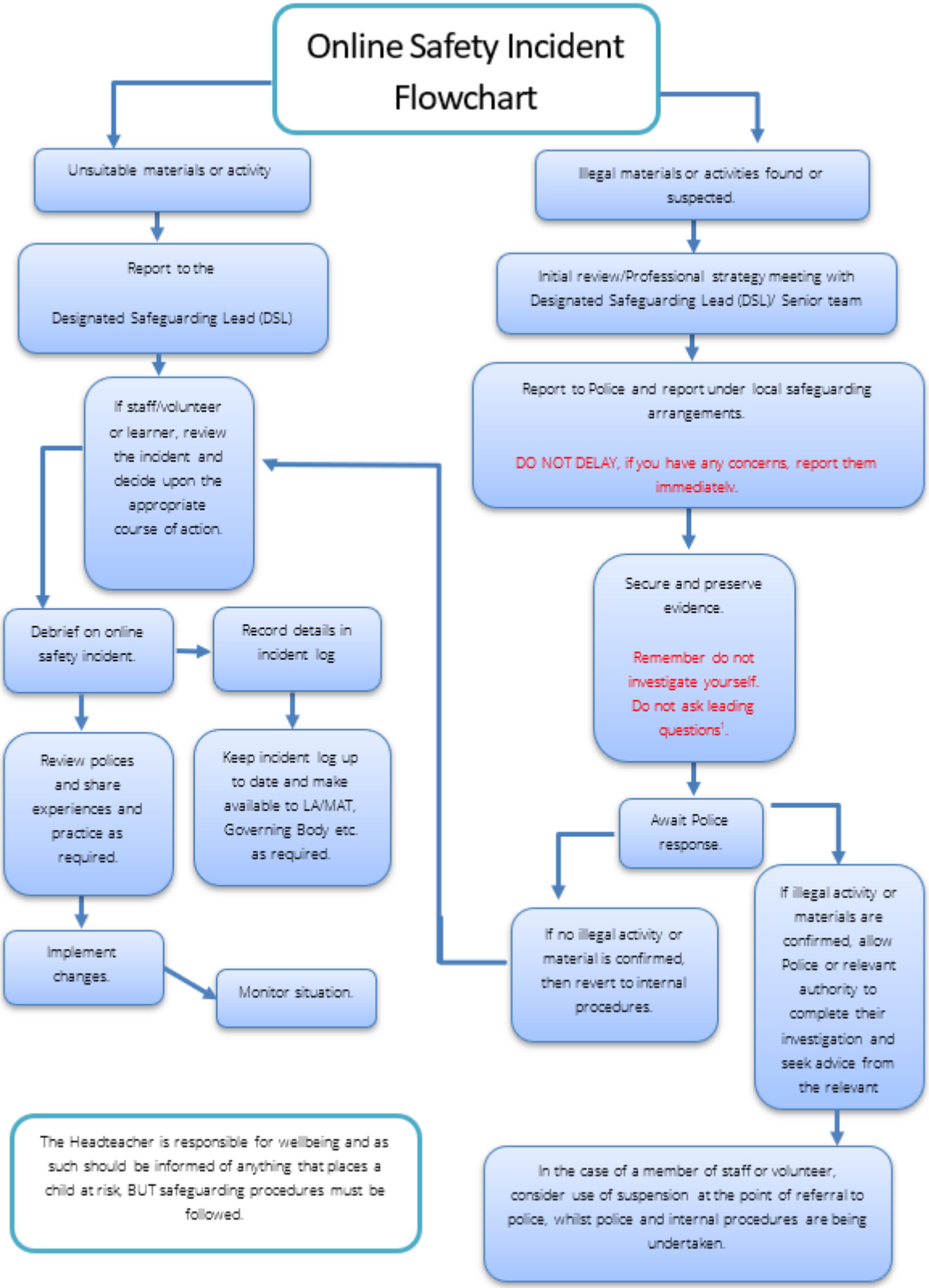
The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all committee members, by agreement of the majority.

The above Terms of Reference for the Grove Learning Trust online safety group have been agreed.

Signed by strategic safeguarding lead for GLT: .....

Date: .....

A6: Responding to incidents of misuse – flow chart



A7: Record of reviewing devices/internet sites (responding to incidents of misuse)

Date: .....

Reason for investigation: .....

.....

.....

Details of first reviewing person

Name: .....
Position: .....
Signature: .....

Details of second reviewing person

Name: .....
Position: .....
Signature: .....

Name and location of computer used for review (for web sites)

.....

.....

Web site(s) address/device	Reason for concern

Conclusion and Action proposed or taken

A8: Reporting Log

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

A9: Training Needs Audit Log

Relevant training the last 12 months	Identified Training Need	To be met by	Cost	Review Date

Legislation

Schools should be aware of the legislative framework under which this online safety policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an online safety issue or situation.

A useful summary of relevant legislation can be found at: Report Harmful Content: Laws about harmful behaviours

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Schools may wish to view the National Crime Agency website which includes information about "Cyber crime – preventing young people from getting involved". Each region in England (& Wales) has a Regional Organised Crime Unit (ROCU) Cyber-Prevent team that works with schools to encourage young people to make positive use of their cyber skills. There is a useful summary of the Act on the NCA site.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

The Data Protection Act 2018:

Updates the 1998 Act, incorporates the General Data Protection Regulations (GDPR) and aims to:

- Facilitate the secure transfer of information within the European Union.
- Prevent people or organisations from holding and using inaccurate information on individuals. This applies to information regarding both private lives or business.
- Give the public confidence about how businesses can use their personal information.
- Provide data subjects with the legal right to check the information businesses hold about them. They can also request for the data controller to destroy it.
- Give data subjects greater control over how data controllers handle their data.
- Place emphasis on accountability. This requires businesses to have processes in place that demonstrate how they're securely handling data.
- Require firms to keep people's personal data safe and secure. Data controllers must ensure that it is not misused.
- Require the data user or holder to register with the Information Commissioner.

All data subjects have the right to:

- Receive clear information about what you will use their data for.
- Access their own personal information.
- Request for their data to be revised if out of date or erased. These are known as the right to rectification and the right to erasure
- Request information about the reasoning behind any automated decisions, such as if computer software denies them access to a loan.
- Prevent or query about the automated processing of their personal data.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes

the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of learners when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

(see template policy in these appendices and for DfE guidance - http://www.education.gov.uk/schools/learnersupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation)

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent/carer to use Biometric systems

The School Information Regulations 2012

Requires schools to publish certain information on its website:

https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

Criminal Justice and Courts Act 2015

Revenge porn – as it is now commonly known – involves the distribution of private and personal explicit images or video footage of an individual without their consent, with the intention of causing them embarrassment and distress. Often revenge porn is used maliciously to shame ex-partners. Revenge porn was made a specific offence in the Criminal Justice and Courts Act 2015. The Act specifies that if you are accused of revenge porn and found guilty of the criminal offence, you could be prosecuted and face a sentence of up to two years in prison.

For further guidance or support please contact the Revenge Porn Helpline

Links to other Organisations

The following links may help those who are developing or reviewing a school online safety policy and creating their online safety provision:

UK Safer Internet Centre

Safer Internet Centre – https://www.saferinternet.org.uk/
South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/
Childnet – http://www.childnet-int.org/
Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
Revenge Porn Helpline - https://revengepornhelpline.org.uk/
Internet Watch Foundation - https://www.iwf.org.uk/
Report Harmful Content - https://reportharmfulcontent.com/
Harmful Sexual Support Service

CEOP

CEOP - http://ceop.police.uk/
ThinkUKnow - https://www.thinkuknow.co.uk/

Others

LGfL – Online Safety Resources
Kent – Online Safety Resources page
INSAFE/Better Internet for Kids - https://www.betterinternetforkids.eu/
UK Council for Internet Safety (UKCIS) - https://www.gov.uk/government/organisations/uk-council-for-internet-safety

Tools for Schools / other organisations

Online Safety BOOST – https://boost.swgfl.org.uk/
360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/
360Data – online data protection self-review tool: www.360data.org.uk
SWGfL Test filtering - http://testfiltering.com/
UKCIS Digital Resilience Framework - https://www.gov.uk/government/publications/digital-resilience-framework
SWGfL 360 Groups – online safety self review tool for organisations working with children
SWGfL 360 Early Years - online safety self review tool for early years organisations

Bullying/Online-bullying/Sexting/Sexual Harassment

Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - http://enable.eun.org/
SELMA – Hacking Hate - https://selma.swgfl.co.uk
Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
Scottish Government - Better relationships, better learning, better behaviour - http://www.scotland.gov.uk/Publications/2013/03/7388

DfE - Cyberbullying guidance -
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf
Childnet – Cyberbullying guidance and practical PSHE toolkit:
http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit
Childnet – Project deSHAME – Online Sexual Harrassment
UKSIC – Sexting Resources
Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm
Ditch the Label – Online Bullying Charity
Diana Award – Anti-Bullying Campaign

Social Networking

Digizen – Social Networking
UKSIC - Safety Features on Social Networks
Children's Commissioner, TES and Schillings – Young peoples' rights on social media

Curriculum

SWGfL Evolve - https://projectevolve.co.uk
UKCCIS – Education for a connected world framework
Department for Education: Teaching Online Safety in Schools

Teach Today – www.teachtoday.eu/
Insafe - Education Resources

Data Protection

360data - free questionnaire and data protection self review tool

ICO Guides for Organisations

IRMS - Records Management Toolkit for Schools

ICO Guidance on taking photos in schools

Professional Standards/Staff Training

DfE – Keeping Children Safe in Education
DfE - Safer Working Practice for Adults who Work with Children and Young People
Childnet – School Pack for Online Safety Awareness
UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure/Technical Support/Cyber-security

UKSIC – Appropriate Filtering and Monitoring
SWGfL Safety & Security Resources
Somerset - Questions for Technical Support
SWGfL - Cyber Security in Schools.

NCA – Guide to the Computer Misuse Act
NEN – Advice and Guidance Notes

Working with parents and carers

SWGfL – Online Safety Guidance for Parents & Carers
Vodafone Digital Parents Magazine
Childnet Webpages for Parents & Carers
Get Safe Online - resources for parents
Teach Today - resources for parents workshops/education
Internet Matters

Prevent

Prevent Duty Guidance
Prevent for schools – teaching resources
Childnet – Trust Me

Research

Ofcom –Media Literacy Research

Version Control

Version	Date	Status	Author (AU) / Approver (AP)
Draft 01	28.03.24	Completion of first draft	AW (AU)
Final – A	23.04.24	Ratified by Standards and Performance (S&P) Committee	S&P Committee
Final B	Autumn 25	Updated to align with KCSiE (PG2)	BG (AU) AW (AP)

Review

Next Review	Spring 2026