Online Safety Policy
2023

DUKE OF NORFOLK CE PRIMARY SCHOOL

This policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, 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 (where allowed).

Version: 1

Date created: 11/10/23

Next review date: 11/10/24

Contents

1 Introduction

The requirement that learners can use digital technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. Schools must, through their Online Safety Policy, meet their statutory obligations to ensure that learners are safe and are protected from potential harm, both on and off-site. It will also form part of the school's protection from legal challenge, relating to the use of digital technologies.

It is best practice that the school reviews their Online Safety Policy at least annually and, if necessary, more frequently in response to any significant new technological developments or trends in technology related behaviours.

Schools in England are subject to an increased level of scrutiny of their online safety practices by Ofsted Inspectors during inspections, while 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.

2 Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of the Duke of Norfolk CE Primary School to safeguard members of our school community online in accordance with statutory guidance and best practice.

This Online Safety Policy applies to all members of the school community (including staff, learners, governors, volunteers, parents and carers, visitors, 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 (where allowed).

The Duke of Norfolk CE Primary School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

3 Policy development, monitoring and review

This Online Safety Policy has been developed by the *school leadership team, DSLs and governing body.*3.1 Schedule for development, monitoring and review

This Online Safety Policy was approved by the *school governing body on:*	*Autumn 2023*
The implementation of this Online Safety Policy will be monitored by:	*The monitoring group: Designated safeguarding leads, online safety lead, senior leadership team, and safeguarding governor*
Monitoring will take place at regular intervals:	*At least once a year*
The *governing body* will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*At least once a year*
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*Autumn 2024*
Should serious online safety incidents take place, the following external persons/agencies should be informed:	*LA safeguarding officer, police*

3.1 Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Filtering and monitoring logs
- Internal monitoring data for network activity
- Surveys/questionnaires of:
    - learners
    - parents and carers
    - staff

4 Policy and Leadership

4.1 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[1] and groups within the school.

4.2 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 Leads, as defined in Keeping Children Safe in Education.
- The Headteacher and (at least) the Deputy Headteacher 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[2].
- The Headteacher/Deputy are responsible for ensuring that the Designated Safeguarding Leads, 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/Deputy 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/Deputy will receive regular monitoring reports from the Designated Safeguarding Leads.
- The Headteacher/Deputy will work with the responsible Governor, the designated safeguarding leads (DSLs) and IT service providers in all aspects of filtering and monitoring.

4.3 Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy e.g. by asking the questions posed in the UKCIS document "Online Safety in Schools and Colleges – questions from the Governing Body". This review will be carried out by the Online Safety Governor who will receive regular information about online safety incidents and monitoring reports. A member of the governing body will take on the role of Online Safety Governor to include:

- **regular meetings with the Designated Safeguarding Leads**
- **regularly receiving (collated and anonymised) reports of online safety incidents**
- **checking that provision outlined in the Online Safety Policy (e.g., online safety education provision and staff training is taking place as intended)**
- **Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually.** (The review will be conducted by members of the SLT, the DSLs, and the IT service provider and involve the responsible governor) - in-line with the DfE Filtering and Monitoring Standards
- **reporting to relevant *governing body meeting***
- Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards
- *membership of the school Online Safety Group*

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

---

[2] See flow chart on dealing with online safety incidents in 'Responding to incidents of misuse' and relevant local authority/MAT/ HR/other relevant body disciplinary procedures.

4.4 Designated Safeguarding Leads (DSLs)

The DSLs 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
- report regularly to headteacher/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)

4.5 Online Safety Lead

The Online Safety Lead will:

- work closely on a day-to-day basis with the Designated Safeguarding Leads (DSLs)
- 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 policies/documents
- 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 / governors/parents/carers/ learners
- liaise with school 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

4.6 Curriculum Leads

Curriculum Leads will work with the DSL/OSL to develop a planned and coordinated online safety education programme e.g. ProjectEVOLVE .

This will be provided through:

- a discrete programme
- PHSE and SRE programmes
- a mapped cross-curricular programme
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

4.7 Teaching and support staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/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 to the DSLs for investigation/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 (where allowed) 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*
- where lessons take place using live-streaming or videoconferencing, there is regard to national safeguarding guidance and local safeguarding policies
- 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.

4.8 IT Provider

As the school has a technology service provided by an outside contractor, it is the responsibility of the school to ensure that the 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 and Technical Security 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 and guidance from the local authority or other relevant body
- 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 to the DSLs 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 updated as agreed in school policies

4.9 Learners

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy. This includes personal devices.
- 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.

4.10 Parents and carers

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 which parents will acknowledge by signature
- publish information about appropriate use of social media relating to posts concerning the school
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

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) and outside school

5 Online Safety Group

The Online Safety Group has the following members:

- Designated Safeguarding Leads/Senior Leaders
- Online Safety Lead/Computing Lead
- Technical staff
- Safeguarding governor

Members of the Online Safety Group will assist the DSL/OSL with:

- the production/review/monitoring of the school Online Safety Policy/documents
- the production/review/monitoring of the school filtering policy and requests for filtering changes

- mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression and coverage
- reviewing network/filtering/monitoring/incident logs, where possible
- encouraging the contribution of learners to staff awareness, emerging trends and the school online safety provision
- consulting stakeholders – including staff/parents/carers about the online safety provision
- monitoring improvement actions identified through use of the 360-degree safe self-review tool.

6 Professional Standards

There is an expectation that required professional standards will be applied to online safety as in other aspects of school life i.e., policies and protocols are in place for the use of online communication technology between the staff and other members of the school and wider community, using officially sanctioned school mechanisms.

7 Policy

7.1 Online Safety Policy

The school 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 (in the induction suite of documents on the secure staff area on the school website)
- *is published on the school website.*

8 Acceptable Use

8.1 Definitions

The school has defined what it regards as acceptable/unacceptable use and this is shown in the tables below.

8.2 Acceptable use agreements

The Online Safety Policy and acceptable use agreements define acceptable use at the school. The acceptable use agreements will be communicated/re-enforced through:

- staff induction
- posters/notices around where technology is used

- communication with parents/carers
- built into education sessions
- school website
- peer support

8.3 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 contain or relate to:	**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 • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering N.B. Schools should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					X
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 (even if the initial access is authorised) • 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

8.3 User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)				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	
	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	

8.4 User Permissions	Staff and Other Adults				Learners			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff/with permission	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission/awareness
Gaming	x							x
Online Shopping/Commerce			x		x			
File Sharing		x						x
Social Media			x		x			
Messaging/Chat			x		x			
Entertainment/Streaming (e.g. Disney+ or Netflix)			x					x
Use of video broadcasting, e.g. YouTube, Twitch, TikTok			x					x
Mobile phones may be brought to school		x						x
Use of mobile phones for learning at school			x		x			

Use of mobile phones in social time at school		x			x			
Taking photos on mobile phones/cameras				x	x			
Use of other personal devices, e.g., tablets, gaming devices			x					
Use of personal e-mail in school, or on school network/wi-fi			x		x			
Use of school e-mail for personal e-mails	x				x			

When using communication technologies, the school 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 should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community
- users should immediately report to a nominated person – in accordance with the school policy – 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.
- relevant policies and permissions should 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.

9 Reporting and Responding

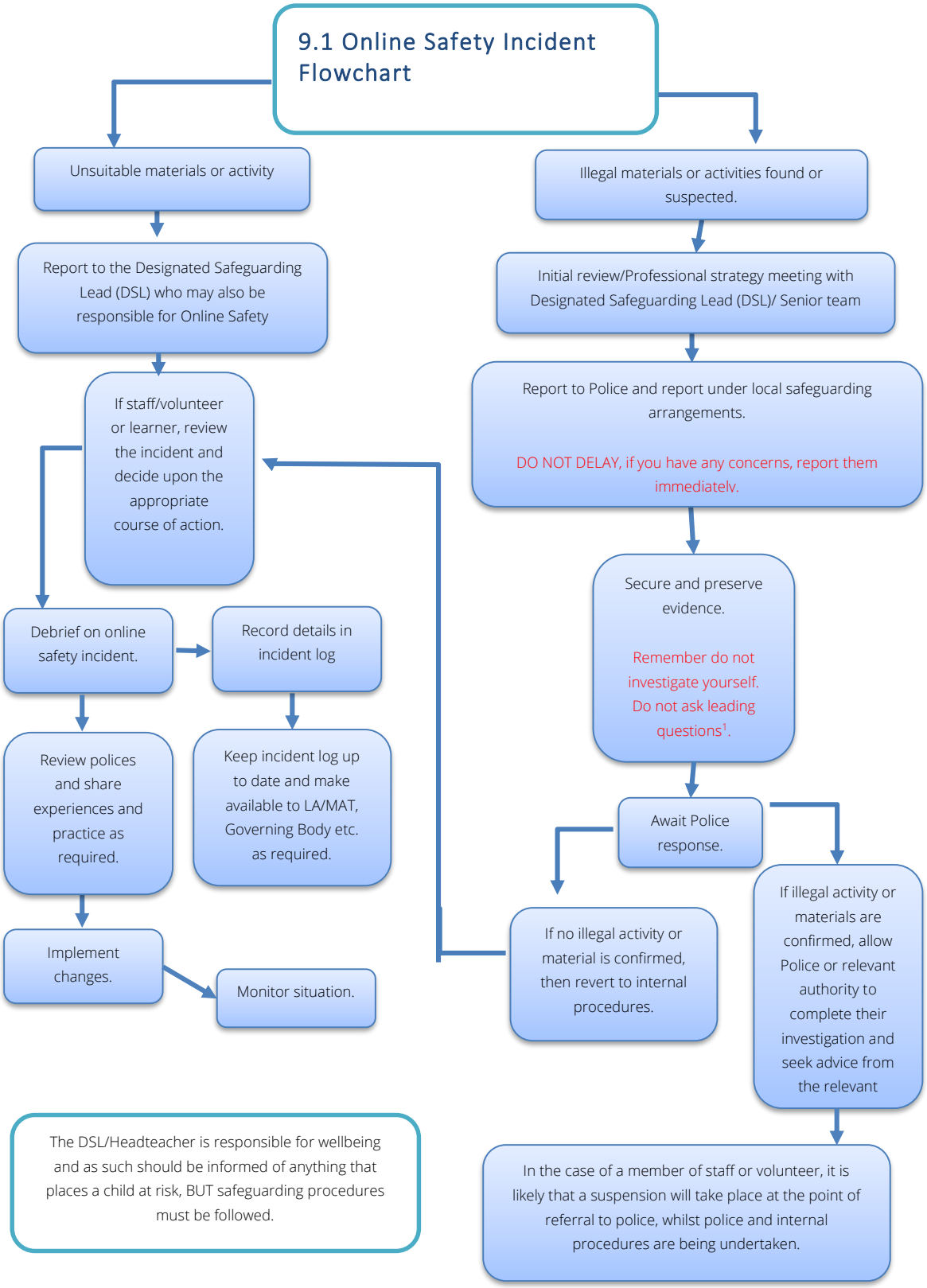
The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- 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 Leads, 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 Chair of Governors and the local authority
- where there is no suspected illegal activity, devices may be checked using the following procedures:
    - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported
    - 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). Use the same device for the duration of the procedure
    - ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection)
    - 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 of the content on the machine being used for investigation. These may be printed, signed, and attached to the form
    - 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
        - police involvement and/or action
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents should be logged on My Concern
- 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 (as relevant)
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
    - *the Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with*
    - *staff, through regular briefings*
    - *learners, through assemblies/lessons*
    - *parents/carers, through newsletters, school social media, website*
    - *governors, through regular safeguarding updates*
    - *local authority/external agencies, as relevant*

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

9.1 Online Safety Incident Flowchart



The DSL/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.

10 School Actions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

10.1 Responding to Learner Actions

Incidents	Refer to class teacher	Refer to Head of Department / Deputy Head	Refer to Headteacher	Refer to Police/Social Care	Refer to local authority technical support for advice/action	Inform parents/carers	Remove device/ network/internet access rights	Issue a warning	Further sanction, in line with behaviour policy
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on User Actions on unsuitable/inappropriate activities).		X	X	X					
Attempting to access or accessing the school network, using another user's account (staff or learner) or allowing others to access school network by sharing username and passwords						X		X	X
Corrupting or destroying the data of other users.			X		X	X			
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature			X			X			
Unauthorised downloading or uploading of files or use of file sharing.			X		X	X			
Using proxy sites or other means to subvert the school's filtering system.			X		X	X			
Accidentally accessing offensive or pornographic material and failing to report the incident.		X			X	X		X	
Deliberately accessing or trying to access offensive or pornographic material.			X			X		X	X

Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.			X			X			X
Unauthorised use of digital devices (including taking images)			X			X		X	X
Unauthorised use of online services		X				X		X	X
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.			X			X			X
Continued infringements of the above, following previous warnings or sanctions.			X			X	X		X

10.2 Responding to Staff Actions

Incidents	Refer to line manager	Refer to Headteacher	Refer to local authority (LADO)/HR	Refer to Police	Refer to LA / Technical Support Staff for action re filtering, etc.	Issue a warning	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)		X	X	X			X
Deliberate actions to breach data protection or network security rules.		X	X	X			X
Deliberately accessing or trying to access offensive or pornographic material		X	X				X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X		X			X
Using proxy sites or other means to subvert the school's filtering system.		X			X	X	
Unauthorised downloading or uploading of files or file sharing		X			X	X	
Breaching copyright or licensing regulations.		X			X	X	
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.		X			X	X	
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature		X	X	X			X
Using personal e-mail/social networking/messaging to carry out digital communications with learners and parents/carers		X					X

Inappropriate personal use of the digital technologies e.g., social media / personal e-mail		X					X
Careless use of personal data, e.g., displaying, holding or transferring data in an insecure manner		X			X		X
Actions which could compromise the staff member's professional standing		X	X				X
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.		X	X				X
Failing to report incidents whether caused by deliberate or accidental actions		X	X			X	
Continued infringements of the above, following previous warnings or sanctions.		X	X				X

11 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.

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 e.g. Education for a Connected Work Framework by UKCIS/DCMS and the SWGfL Project Evolve 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.
- it 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. Lessons and further resources are available on the CyberChoices site
- staff should act as good role models in their use of digital technologies the internet and mobile devices
- 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, students may need to research topics, (e.g., racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to 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

11.1 Contribution of Learners

The school acknowledges, learns from, and uses the skills and knowledge of learners in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the school community and how this contributes positively to the personal development of young people. Their contribution is recognised through:

- mechanisms to canvass learner feedback and opinion.
- appointment of digital leaders/anti-bullying ambassadors
- the Online Safety Group has learner representation
- learners contribute to the online safety education programme e.g., peer education, digital leaders leading lessons for younger learners, online safety campaigns
- learners designing/updating acceptable use agreements
- contributing to online safety events with the wider school community e.g., parents' evenings, family learning programmes etc.

11.2 Staff/Volunteers

All staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- a planned programme of formal online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- the training will be an integral part of the school's annual safeguarding and data protection training for all staff
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours.

- the Online Safety Lead and Designated Safeguarding Lead will receive regular updates through attendance at external training events, (e.g. UKSIC / SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations
- this Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days
- the Designated Safeguarding Leads/Online Safety Lead will provide advice/guidance/training to individuals as required.

11.3 Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members involved in technology/online safety/health and safety/safeguarding. This may be offered in several ways such as:

- attendance at training provided by the local authority/MAT or other relevant organisation (e.g., DCC)
- participation in school training / information sessions for staff or parents

A higher level of training will be made available to (at least) the Online Safety Governor. This will include:

- Cyber-security training (at least at a basic level)
- Training to allow the governor to understand the school's filtering and monitoring provision, in order that they can participate in the required checks and review.

11.4 Families

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will seek to provide information and awareness to parents and carers through:

- regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes
- regular opportunities for engagement with parents/carers on online safety issues through awareness workshops / parent/carer evenings etc.
- the learners – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by learners leading sessions at parent/carer evenings.
- letters, newsletters, website, learning platform,
- high profile events / campaigns e.g., Safer Internet Day
- reference to the relevant web sites/publications, e.g. SWGfL; www.saferinternet.org.uk/; www.childnet.com/parents-and-carers (see Appendix for further links/resources).
- Sharing good practice with other schools in clusters and or the local authority

11.5 Adults and Agencies

The school will provide opportunities for local community groups and members of the wider community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- online safety messages targeted towards families and relatives.
- *providing family learning courses in use of digital technologies and online safety*
- *providing online safety information via their website and social media for the wider community*

12 Technology

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

13 Filtering & Monitoring

The school filtering and monitoring provision is agreed by senior leaders, governors and the IT Service Provider and is 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 DSLs will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility.

The filtering and monitoring provision is reviewed (at least annually) by senior leaders, the Designated Safeguarding Leads, and a governor, 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 a senior leader, the Designated Safeguarding Leads and a governor, in particular when a safeguarding risk is identified, there is a change in working practice, e.g., remote access or BYOD or new technology is introduced.

13.1 Filtering

- the school manages access to content across its systems for all users and on all devices using the school's 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 5).
- filtering logs are regularly reviewed and alert the Designated Safeguarding Leads to breaches of the filtering policy, which are then acted upon.
- younger learners will use child friendly/age-appropriate search engines e.g. SWGfL Swiggle
- the school has a mobile phone policy and where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice
- access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

13.2 Monitoring

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

- The school monitors all network use across all its devices and services
- monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Leads, 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 informed by the school's risk assessment. These may include:

- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed, and breaches are reported to senior leaders
- *pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.*
- *where possible, school technical staff regularly monitor and record the activity of users on the school technical systems*
- *use of a third-party assisted monitoring service to review monitoring logs and report issues to school monitoring lead(s)*

13.3 Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements:

- responsibility for technical security resides with SLT who may delegate activities to identified roles
- all users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the IT service provider and will be reviewed, at least annually, by the SLT/Online Safety Group
- password policy and procedures are implemented consistent with guidance from the National Cyber Security Centre
- the security of their username and password and must not allow other users to access the systems using their log on details
- all users have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details
- all school networks and system will be protected by secure passwords. Passwords must not be shared with anyone
- the administrator passwords for school systems are kept in a secure place, e.g., school safe
- there is a risk-based approach to the allocation of learner usernames and passwords
- there will be regular reviews and audits of the safety and security of school technical systems
- servers, wireless systems and cabling are securely located and physical access restricted
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint software

- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,
- the school administration team is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied
- an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed
- use of school devices out of school and by family members is regulated by an acceptable use statement that a user consents to when the device is allocated to them
- personal use of any device on the school network is regulated by acceptable use statements that a user consents to when using the network
- staff members are not permitted to install software on a school-owned devices without the consent of the SLT/IT service provider
- removable media is not permitted unless approved by the SLT/IT service provider
- systems are in place to control and protect personal data and data is encrypted at rest and in transit
- mobile device security and management procedures are in place (where mobile devices are allowed access to school systems)
- guest users are provided with appropriate access to school systems based on an identified risk profile.

13.4 Mobile technologies

The school acceptable use agreements for staff, learners, parents, and carers 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[3]	Student owned	Staff owned	Visitor owned
Allowed in school	X	X	X	X	X	X
Full network access	X	X	X			
Internet only					X	X
No network access				X		

School owned

- there is an asset log that clearly states whom a device has been allocated to. There is clear guidance on where, when and how use is allowed

[3] 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.

- any designated mobile-free zone is clearly signposted
- personal use (e.g. online banking, shopping, images etc.) is clearly defined and expectations are well-communicated.
- the use of devices on trips/events away from school is clearly defined and expectation are well-communicated.
- liability for damage aligns with current school policy for the replacement of equipment.
- education is in place to support responsible use.

Personal devices:

- there is a clear policy covering the use of personal mobile devices on school premises for all users
- where devices are used to support learning, staff have been trained in their planning, use and implementation, ensuring that all learners can access a required resource
- where personal devices are brought to school, but their use is not permitted, appropriate, safe and secure storage should be made available.
- use of personal devices for school business is defined in the acceptable use policy. Personal devices commissioned onto the school network are segregated effectively from school-owned systems
- the expectations for taking/storing/using images/video aligns with the school's acceptable use policy and use of images/video policy. The non-consensual taking/using of images of others is not permitted.
- liability for loss/damage or malfunction of personal devices is clearly defined
- there is clear advice and guidance at the point of entry for visitors to acknowledge school requirements
- education about the safe and responsible use of mobile devices is included in the school online safety education programmes

14 Social Media

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
- risk assessment, including legal risk
- 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
- a code of behaviour for users of the accounts

- systems for reporting and dealing with abuse and misuse
- understanding of how incidents may be dealt with under school disciplinary procedures.

14.1 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*

14.2 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
- the school should effectively respond to social media comments made by others according to a defined policy or process
- 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 the Online Safety Lead to ensure compliance with the social media, data protection, communications, digital image and video policies. In the event of any social media issues that the school is unable to resolve support may be sought from the Professionals Online Safety Helpline.

15 Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and learners need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies. Guidance can be found on the SWGfL Safer Remote Learning web pages and in the DfE Safeguarding and remote education
- when using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.

- staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes
- in accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other learners in the digital/video images
- staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images
- care should be taken when sharing digital/video images that learners are appropriately dressed
- learners must not take, use, share, publish or distribute images of others without their permission
- photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with Online Safety Policy
- learners' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- written permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media.
- parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy
- images will be securely stored in line with the school retention policy
- learners' work can only be published with the permission of the learner and parents/carers.

16 Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through:

- Public-facing website
- Social media (Facebook/Twitter)
- Online newsletters
- Seesaw App
- Google Classrooms
- Text Messages (Teachers2Parents)

The school website is hosted by Primary Site. The school ensures that online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.

Where learner work, images or videos are published, their identities are protected, and full names are not published.

The school public online publishing provides information about online safety e.g., publishing the schools Online Safety Policy and acceptable use agreements; curating latest advice and guidance; news articles etc., creating an online safety page on the school website.

17 Data Protection

Personal data will be recorded, processed, transferred, and made available according to the current data protection legislation.

The school:

- has a Data Protection Policy
- implements the data protection principles and can demonstrate that it does so
- has paid the appropriate fee to the Information Commissioner's Office (ICO)
- has appointed an appropriate Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest.
- has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- the Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed
- has an 'information asset register' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed
- will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school 'retention schedule" supports this
- data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- provides staff, parents, volunteers, teenagers, and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice
- has procedures in place to deal with the individual rights of the data subject, e.g., one of the dozen rights applicable is that of Subject Access which enables an individual to see/have a copy of the personal data held about them
- carries out Data Protection Impact Assessments (DPIA) where necessary e.g., to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier
- has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors
- understands how to share data lawfully and safely with other relevant data controllers.
- has clear and understood policies and routines for the deletion and disposal of data
- reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents
- has a Freedom of Information procedures which sets out how it will deal with FOI requests
- provides data protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff

When personal data is stored on any mobile device or removable media the:

- data will be encrypted, and password protected.
- device will be password protected
- device will be protected by up-to-date endpoint (anti-virus) software
- data will be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Staff must ensure that they:

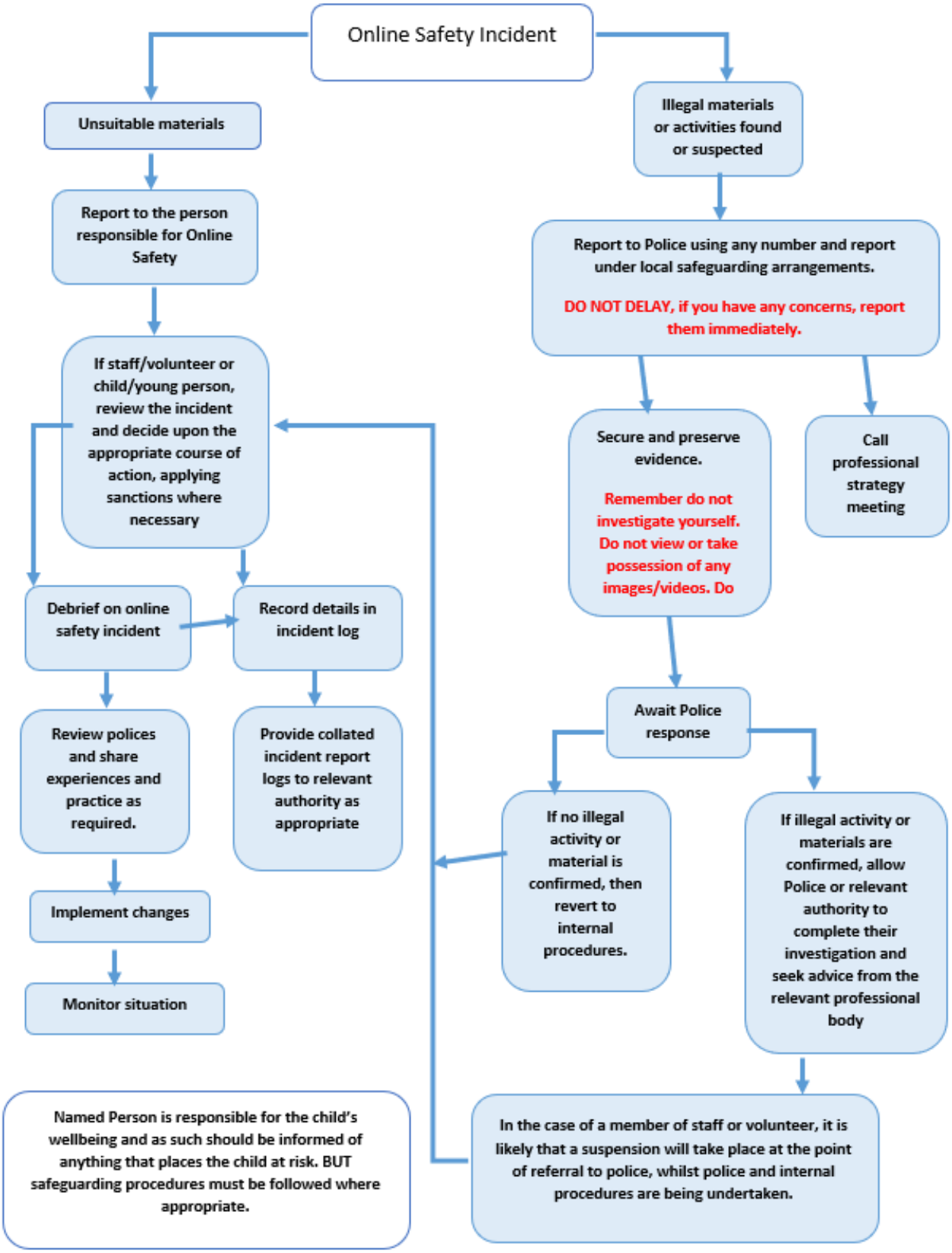
- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school
- only use encrypted data storage for personal data
- will not transfer any school personal data to personal devices. Procedures should be in place to enable staff to work from home (i.e., a work laptop provided)
- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
- transfer data using encryption, a secure email account (where appropriate), and secure password protected devices

18 Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, learners; parents/carers and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors
- parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
- the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.

Appendix 1 Responding to incidents of misuse – flow chart



Appendix 2 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.

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

Appendix 3: Links to other organisations or documents

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/
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

Ofsted: Review of sexual abuse in schools and colleges

Further links can be found at the end of the UKCIS Education for a Connected World Framework

Appendix 4 – Filtering Incident Reporting Log

Class:

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

Appendix 5 – Staff Request for specific website unblocking

Staff name and year group/department:

Website title and URL/link:

Year group you want the website unblocked for (if applicable):

Reason why you want the website unblocked:

E.g. students need to access it for classwork, homework, revision

Can we re-block this site after a specific date?

No ☐

Yes ☐ Date the website can be re-blocked: _____

Appendix 6 – Filtering Monitoring Review

The review should be done as a minimum termly, or when:
- a safeguarding risk is identified
- there is a change in working practice, like remote access or BYOD
- new technology is introduced

MONITORING CHECKS FORM	DATE OF CHECK	WHO DID THE CHECK	NOTES/RESULTING ACTIONS
Have we checked that our filtering and monitoring system is still fit for purpose? (Results of South West Grid for Learning's (SWGfL) testing tool)			
Is the system running and working?			
Is our filtering and monitoring system working on: › All devices? › New devices and services before they're given to staff or pupils?			
Have we reviewed the list of blocked sites on our network? Is this list still accurate/does it reflect any changes to safeguarding risks?			
Does our filtering system adhere to the following requirements**?** **Has the filtering checklist been completed (annually)?**			
Does our monitoring system adhere to the requirements? **Has the monitoring checklist been completed (annually)?**			

Appendix 7 – Annual Filtering Checklist

The review should be done as a minimum **annually,** or when:

- a safeguarding risk is identified
- there is a change in working practice, like remote access or BYOD
- new technology is introduced

REQUIREMENTS - FILTERING SYSTEM	✓
Is it a member of the Internet Watch Foundation (IWF)?	☐
Is it signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)?	☐
Does it block access to illegal content including child sexual abuse material (CSAM)?	☐
Are you satisfied that the system manages the following content: › Discrimination › Drugs/substance abuse › Extremism › Gambling › Malware/hacking › Pornography › Piracy and copyright theft › Self harm › Violence	☐
Is the filtering system: › Operational › Up to date › Applied to all: o Users, including guest accounts o School-owned devices o Devices using the school broadband connection	☐
Does the filtering system: › Filter all internet feeds, including any backup connections › Handle multilingual web content, images, common misspellings and abbreviations › Identify technologies and techniques that allow users to get around the filtering, such as VPNs and proxy services, and block them › Provide alerts when any web content has been blocked It is: › Age and ability appropriate for the users, and suitable for educational settings	☐
Does the filtering system allow you to identify: › Device name or ID, IP address, and where possible, the individual › The time and date of attempted access › The search term or content being blocked	☐
Are you clear on how long logfile information (internet history) is retained and how it's stored?	☐
Are you clear on how the system does not over block access so it doesn't lead to unreasonable restrictions?	☐

REQUIREMENTS - FILTERING SYSTEM	✓
Does the filtering system meet the following principles? › Context appropriate differentiated filtering, based on age, vulnerability and risk of harm o Can you vary the filtering strength? E.g. for staff? › Circumvention o Can you identify and manage technologies used to circumvent the system, e.g. virtual personal networks (VPNs), proxy services and domain name system (DNS) over Hypertext Transfer Protocol Secure (HTTPS) › Control o Can you control the filter yourselves to permit or deny specific content? o Can you log any changes as part of an audit trail? › Contextual content filters o In addition to URL or IP-based filtering, the extent to which (http and https) content is analysed as it is streamed to the user and blocked, this would include artificial intelligence (AI) generated content. For example, being able to contextually analyse text on a page and dynamically filter › Filtering Policy o Does your provider detail its approach to filtering, as well as over blocking? › Group/multi-site management o Can your system be deployed centrally, with a central policy and dashboard? › Identification o Does the system allow you to identify users? › Multiple language support o Does the system manage relevant languages? › Network level o Is the filtering provided at 'network level', i.e. it doesn't reply on software on user devices while at school	☐
› Remote devices o Can the system filter devices where staff and/or pupils are working remotely? › Reporting o Can you report inappropriate content? o Does the system provide clear historical information on the websites users have accessed or tried to access? › Safe Search o Does the system have the ability to enforce 'safe search'?	☐
If users access content via mobile or through apps: Get confirmation that your provider can provide filtering on mobile or app technologies. They should also apply a technical monitoring system to devices using mobile and app content to reduce the risk of harm.	☐
If your filtering provision is procured with a broadband service: Make sure it meets the needs of your school or college	☐

Appendix 8 – Annual Monitoring Checklist

The review should be done as a minimum **annually,** or when:

The review should be done as a minimum **annually,** or when:

- a safeguarding risk is identified
- there is a change in working practice, like remote access or BYOD
- new technology is introduced

REQUIREMENT - MONITORING SYSTEM	✓
Are incidents urgently picked up, acted on and the outcomes recorded?	☐
Are all staff clear on: › How to deal with these incidents? › Who should lead on any actions?	☐
Is device monitoring managed? (this could be by your IT staff or a third-party provider) Whoever is managing device monitoring will need to: › Make sure monitoring systems are working as expected › Provide reports on pupil device activity › Receive safeguarding training including online safety › Record and report safeguarding concerns to the DSL	☐
Is your monitoring data received in a format that your staff can understand?	☐
Are users identifiable to your school or college, so you can trace concerns to an individual, including guest accounts?	☐
Does your monitoring system alert you to behaviours associated with: › Content o Being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism › Contact o 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 o Online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying › Commerce o Risks such as online gambling, inappropriate advertising, phishing and/or financial scams	☐

REQUIREMENT - MONITORING SYSTEM	✓
Does the monitoring system meet the following principles: › Age appropriate o Can you vary your system to take age, vulnerability, or specific situations into account? › Audit trail o Are any changes to the monitoring system logged so no one can make changes on their own usage? › Data retention o Are we clear on what data is stored, where and for how long (including any backup data)? › Devices o Is our monitoring system is clear about which devices it covers? › Flexibility o Is it clear how keywords can be added or removed? › Group/multi-site management o Can your strategy be deployed centrally, with a central policy and dashboard? › Harmful image detection o To what extent is visual content monitored and analysed? › Impact o How do monitoring results impact your policy and practice?	☐
› Monitoring policy o Do you tell all users that you're monitoring their online access? o Do you communicate your expectations on appropriate use to pupils and staff? › Multiple language support o Can the system manage relevant languages in your school? › Prioritisation o How are alerts prioritised? o What procedures do you have in place to allow staff to respond to alerts rapidly? › Remote monitoring o Can the system monitor devices where staff and/or pupils are working remotely? o Are users aware of this? Are you clear if these devices are only monitored during school hours? › Reporting o How are alerts recorded, communicated and escalated?	☐
Do your staff: › Provide effective supervision? › Take steps to maintain awareness of how devices are being used by pupils? › Report any safeguarding concerns to the DSL?	☐