



and



Abbots Farm Preschool

Online Safety Policy

December 2022

Review by December 2023

Contents:

Statement of intent

1. [Legal framework](#)
2. [Roles and responsibilities](#)
3. [Online Safety Policy Aims](#)
4. [Acceptable Use](#)
5. [Reporting and Responding](#)
6. [School Actions](#)
7. [Online Safety Education Programme](#)
8. [Contribution of Children](#)
9. [Staff and Volunteers](#)
10. [Governors](#)
11. [Families](#)
12. [Remote Learning](#)
13. [Technology](#)
14. [Filtering](#)
15. [Monitoring](#)
16. [Technical Security](#)
17. [Social Media](#)
18. [Digital and Video Images](#)
19. [Online Publishing](#)
20. [Data Protection](#)
21. [Monitoring and review](#)

Appendices

1. Responding to incidents of misuse – flow chart
2. Record of reviewing devices/internet sites (responding to incidents of misuse)
3. Reporting Log
4. Training Needs Audit Log
5. Links to other organisations or documents

Statement of intent

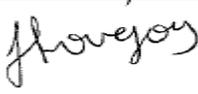
Abbots Farm Infant School and Abbots Farm Preschool understand that using online services is an important aspect of raising educational standards, promoting achievement, and enhancing teaching and learning.

We want our children to be able to understand and apply the key skills of computing.

Our children will develop skills enabling them to embrace a digital world. These include the knowledge and abilities to communicate in a variety of ways, solve problems logically and create and correct algorithms, using a wide range of digital technology, whilst knowing how to keep themselves safe online.

The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of children and staff.

Signed by:

	Online Safety Lead	Date: 6/12/22
	Headteacher	Date: 6/12/22
	Chair of governors	Date: 6/12/22

1. Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2022) 'Keeping children safe in education 2022'
- DfE (2019) 'Teaching online safety in school'
- DfE (2018) 'Searching, screening and confiscation'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'

This policy operates in conjunction with the following school policies and procedures:

- Anti-Bullying Policy
- Behaviour and Relationships Policy
- Confidentiality Policy
- Data Protection Policy
- Low-level Safeguarding Concerns Policy
- PSHE and RSHE Policy
- Pupil Remote Learning Plan
- Safeguarding and Child Protection Policy
- Staff Code of Conduct
- Technology Acceptable Use Agreement for Pupils
- Technology Acceptable Use Agreement – Staff
- Whistleblowing Policy

2. Roles and responsibilities

The **Governing Body** is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that all relevant school policies have an effective approach to planning for and responding to, online challenges and hoaxes embedded within them.
- Appointing an online safety Governor to meet regularly with the online safety Lead to monitor online safety incident and filtering logs and report to the governing body.

The **Headteacher and Senior Leaders** are responsible for:

- 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 may be delegated to the Online Safety Lead.
- 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 and senior leaders are responsible for ensuring that the Online Safety Lead, 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 and senior leaders 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 and senior leaders will receive regular monitoring reports from the Online Safety Lead.

The **Online Safety Lead** is responsible for:

- Being a DSL and being trained in online safety issues and being aware of the potential for serious safeguarding issues to arise from:
 - sharing of personal data
 - access to illegal/inappropriate materials
 - inappropriate online contact with adults/strangers
 - potential or actual incidents of grooming
 - online bullying.
- Taking day-to-day responsibility for online safety issues, and being aware of the potential for serious child protection concerns.
- Having a leading role in establishing and reviewing the school online safety policies and documents.
- Promoting an awareness of and commitment to online safety education and awareness raising across the school and beyond.
- Liaising with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated.
- Ensuring 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.
- Receiving reports of online safety incidents and creating a log of incidents to inform future online safety developments.
- Providing (or identifying sources of) training and advice for staff, governors, parents/carers and learners.
- Liaising with WCC technical staff.
- Meeting regularly with the online safety governor to discuss current issues, review (anonymised) incidents and if possible, filtering and monitoring logs.
- Attending relevant governing body meetings.
- Reporting regularly to the Headteacher and senior leadership team.
- Liaising with the local authority.

Curriculum leads are responsible for:

- Working with the Online Safety Lead to develop a planned and coordinated online safety education programme. This will be provided through:
 - A discrete online safety programme
 - A mapped cross-curricular programme
 - PSHE and RSHE programmes such as Jigsaw
 - Assemblies and pastoral programmes
 - Relevant national initiatives and opportunities e.g. [Safer Internet Day](#) and [Anti-bullying week](#).

All **staff members** are responsible for ensuring:

- 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 to the **Headteacher** for investigation and action, in line with the school safeguarding procedures. If they suspect the Headteacher of misuse this must be reported to the **Chair of Governors** immediately.
- All digital communications with learners and parents/carers should be 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.
- 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, iPads, 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 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.
- They have 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.

Technical Support Staff from WCC supported by Online Safety Lead are responsible for ensuring that:

- They are aware of and follow the school Online Safety Policy and 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 local authority.
- 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 and attempted misuse can be reported to the **Headteacher** 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 software and systems are implemented and regularly updated as agreed in school policies.

Children are responsible for:

- Using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement and Online Safety Policy.
- Understanding the importance of reporting abuse, misuse or access to inappropriate materials and knowing how to do so.
- Knowing what to do if they or someone they know feels vulnerable when using online technology.
- Understanding the importance of adopting good online safety practice when using digital technologies out of school and realising 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 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
- Publishing information about appropriate use of social media relating to posts concerning the school
- Seeking their permissions concerning digital images, cloud services etc.
- Parents' and carers' evenings, newsletters, website, social media and information about national and local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- ClassDojo and other on-line apps used for pupil records

3. Online Safety Policy Aims

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 and 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 is on the OneDrive.
- Is published on the school website.

4. Acceptable Use

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

The Online Safety Policy and acceptable use agreements define acceptable use at the school. The acceptable use agreements will be communicated and reinforced through:

- Staff induction and handbook
- Posters and notices around where technology is used
- Communication with parents and carers
- Integration into education sessions
- School website
- Peer support through the E-Safety Council

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:	<p>Any illegal activity for example:</p> <ul style="list-style-type: none"> • Child sexual abuse imagery • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images e.g., 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 					X
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	<ul style="list-style-type: none"> • 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
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 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	

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 children 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.

Consideration should be given for the following activities when undertaken for non-educational purposes:	Staff and other adults				Children			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission/awareness
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		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			

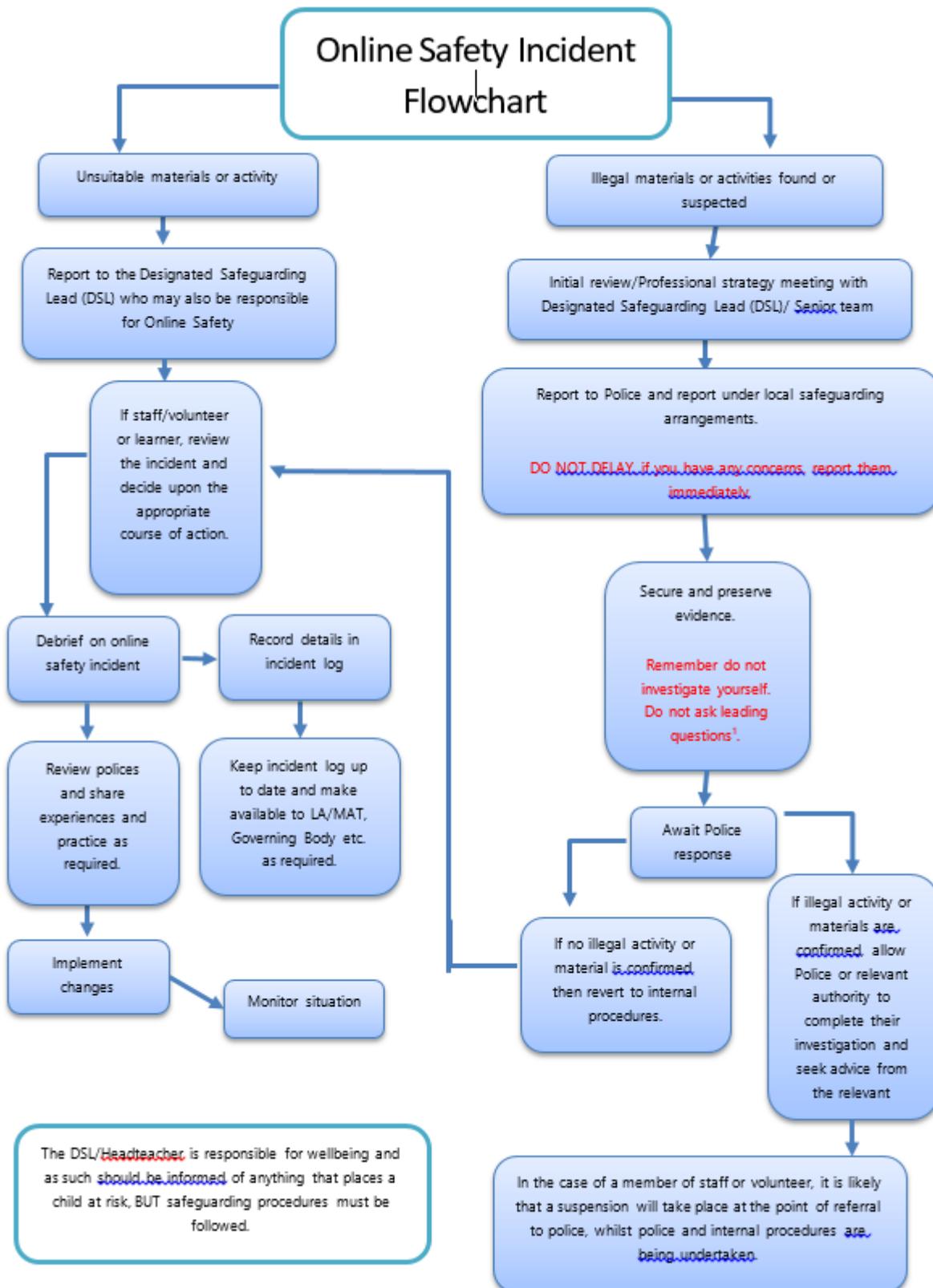
5. Reporting and Responding

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 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.
- 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.
- Where there is no suspected illegal activity, devices can 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 (Appendix 2)
 - 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
- 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 will be logged ([See Reporting Log Appendix 3](#)).
- 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 Senior Leadership Team for consideration of updates to policies or education programmes and to review how effectively the report was dealt with
 - staff, through regular briefings
 - children, 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.



6. 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 procedures as follows:

6.1 Responding to Learner Actions

Incidents	Refer to class teacher	Refer to Headteacher	Refer to Police	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		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		X	X	X	X
Unauthorised downloading or uploading of files or use of file sharing.	X							
Using proxy sites or other means to subvert the school's filtering system.		X	X	X	X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident.		X						
Deliberately accessing or trying to access offensive or pornographic material.		X	X	X	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	X	X	X	X

Unauthorised use of digital devices (including taking images)	X							
Unauthorised use of online services	X							
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.		X			X	X	X	X
Continued infringements of the above, following previous warnings or sanctions.			X			X		X

6.2 Responding to Staff Actions

Incidents	Refer to Headteacher	Refer to local authority	Refer to Police	Refer to LA / Technical Support Staff for action re filtering, etc.	Issue a warning	Suspension	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			X
Deliberate actions to breach data protection or network security rules.	X	X	X	X			X
Deliberately accessing or trying to access offensive or pornographic material		X	X	X			X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X				X
Using proxy sites or other means to subvert the school's filtering system.	X	X		X			X
Unauthorised downloading or uploading of files or file sharing	X			X	X		X
Breaching copyright or licensing regulations.	X	X	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	X				X
Inappropriate personal use of the digital technologies e.g. social media / personal e-mail	X			X	X		X

Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner	X	X			X		X
Actions which could compromise the staff member's professional standing	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
Failing to report incidents whether caused by deliberate or accidental actions	X						X
Continued infringements of the above, following previous warnings or sanctions.	X	X	X			X	X

7. Online Safety Education Programme

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 using Purple Mash 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.
- Children's needs and progress are addressed through effective planning and assessment.
- Digital competency is planned and effectively delivered through other curriculum areas e.g. PSHE; English etc.
- It incorporates use of relevant national initiatives and opportunities e.g. [Safer Internet Day](#) and [Anti-bullying week](#).
- The programme will be accessible to children at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- Children should be helped to understand the need for the pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school.
- 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 children 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 children 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.
- The online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

8. Contribution of Children

The school acknowledges, learns from, and uses the skills and knowledge of children 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
- The appointment of an E-Safety Council
- Children contributing to the online safety education programme e.g. peer education, E-Safety Council leading lessons for younger learners, online safety campaigns
- E-Safety Council reviewing acceptable use agreements
- Contributing to online safety events with the wider school community e.g. assemblies

9. Staff and 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 will receive regular updates through attendance at external training events, 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 meetings.
- The Online Safety Lead will provide advice, guidance and training to individuals as required.

10. Governors

Governors should take part in online safety training and awareness sessions, with particular importance for those who are involved in technology and online safety, health and safety and safeguarding.

This may be offered in several ways such as:

- Attendance at training provided by the local authority.
- Participation in school training and information sessions for staff or parents.

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

11. Families

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 and carers on online safety issues through awareness workshops and ClassDojo posts.
- The children – who are encouraged to pass on to parents the online safety messages they have learned in lessons.
- Letters, newsletters, website.
- High profile events and campaigns e.g. [Safer Internet Day](#).
- Reference to the relevant websites and publications, e.g. [SWGfl](#); www.saferinternet.org.uk/; www.childnet.com/parents-and-carers (see Appendix 5 for further links/resources).
- Sharing good practice with other schools in our Consortium and Soft Federation.

12. Remote Learning

All remote learning is delivered in line with the school's Pupil Remote Learning Plan.

The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use. The school will consult with parents prior to the period of remote learning about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.

The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

During the period of remote learning, the school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.

The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.

13. Technology

The school is responsible for ensuring that the school infrastructure and 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.

14. Filtering

- The school filtering policies are agreed by senior leaders and WCC technical staff and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents and behaviours.
- The school manages access to content across its systems for all users. The filtering provided meets the standards defined in the UK Safer Internet Centre [Appropriate filtering](#).
- Access to online content and services is managed for all users.
- Illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC 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.
- There is a clear process in place to deal with requests for filtering changes.
- Younger learners will use child friendly and age-appropriate search engines e.g. [SWGfL Swiggle](#)
- Filtering logs are regularly reviewed and alert the school to breaches of the filtering policy, which are then acted upon.
- 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.

If necessary, the school will seek advice from, and report issues to, the SWGfL [Report Harmful Content](#) site.

15. 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.
- An appropriate monitoring strategy for all users has been agreed and users are aware that the network is monitored. There is a staff lead responsible for managing the monitoring strategy and processes.
- 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.
- Technical monitoring systems are up to date and managed and logs and alerts are regularly reviewed and acted upon.

The school follows the UK Safer Internet Centre [Appropriate Monitoring](#) guidance and protects users and school systems through the use of:

- Physical monitoring (adult supervision in the classroom)
- Logging of internet use, which is regularly monitored and reviewed
- A third-party assisted monitoring service to review monitoring and filtering logs and report issues to headteacher

16. Technical Security

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

- 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.
- There are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud.
- 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 Network Manager (or other person) and will be reviewed, at least annually, by the Senior Leadership Team.
- All users (adults and learners) 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. Users must immediately report any suspicion or evidence that there has been a breach of security.
- All school networks and system will be protected by secure passwords. Passwords must not be shared with anyone. All users will be provided with a username and password by Lydia Mortimer (School Business Manager) who will keep an up-to-date record of users and their usernames
- The master account passwords for the school systems are kept in a secure place.
- Passwords should be at least 8 characters long and contain upper and lower case letters, digits and symbols.
- Records of learner usernames and passwords for learners in Key Stage 1 or younger can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user.
- Jeanette Lovejoy (Headteacher) 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 or potential technical incident or security breach to the Headteacher.
- 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 (anti-virus) software.

- Lydia Mortimer (School Business Manager) will set up temporary access of 'guests', (e.g., trainee teachers, supply teachers, visitors) onto the school systems. Jeanette Lovejoy (Headteacher) will give access to programmes needed to do their job.
- An agreement is in place regarding the extent of personal use that users (staff and children) and their family members are allowed on school devices that may be used out of school.
- Staff must seek permission from headteacher before downloading executable files and installing programmes on school devices.
- Staff are allowed to use removable media (e.g., memory sticks/CDs/DVDs) on school devices. Where possible these should be encrypted.
- Systems are in place that prevent the unauthorised sharing of personal data unless safely encrypted or otherwise secured. (See Data Protection Policy for further details).

17. Social Media

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

- Ensuring that personal information is not published
- Education and training being provided including acceptable use, age restrictions, social media risks, use of digital and video images, checking of settings, data protection and reporting issues
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Guidance for children, parents and carers

School staff should ensure that:

- No reference should be made in social media to children, 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

On official school social media accounts, there is:

- 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.

17.1 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 upon 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.

17.2 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.

18. Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and children instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and children 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.

- When using digital images, staff will inform and educate children about the risks associated with the taking, use, sharing, publication and distribution of images.
- Staff/volunteers must be aware of those children 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 photographs of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published on social networking sites.
- Staff 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 children are appropriately dressed.
- Children must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include children will be selected carefully and will comply with Online Safety Policy.
- Children's full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission is obtained from parents/carers on School Enrolment Forms to allow photographs of children to be 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.

19. Online Publishing

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

- Public-facing website
- ClassDojo

- Online newsletters

The school website is managed/hosted by Joomla. The school ensures that the 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 children's work, images or videos are published, their identities are protected, and full names are not published.

On the schools website there is an E-Safety page which provides information about online safety e.g., Online Safety Policy and acceptable use agreements; curating latest advice and guidance; news articles etc.

20. 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) through Warwickshire's DPO Service who has effective understanding of data protection law and is free from any conflict of interest. Our Data Controllers are Jeanette Lovejoy (Headteacher) and Lydia Mortimer (School Business Manager).
- 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. The 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, governors and volunteers, 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.
- 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 Policy 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 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.
- 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.

21. Monitoring and review

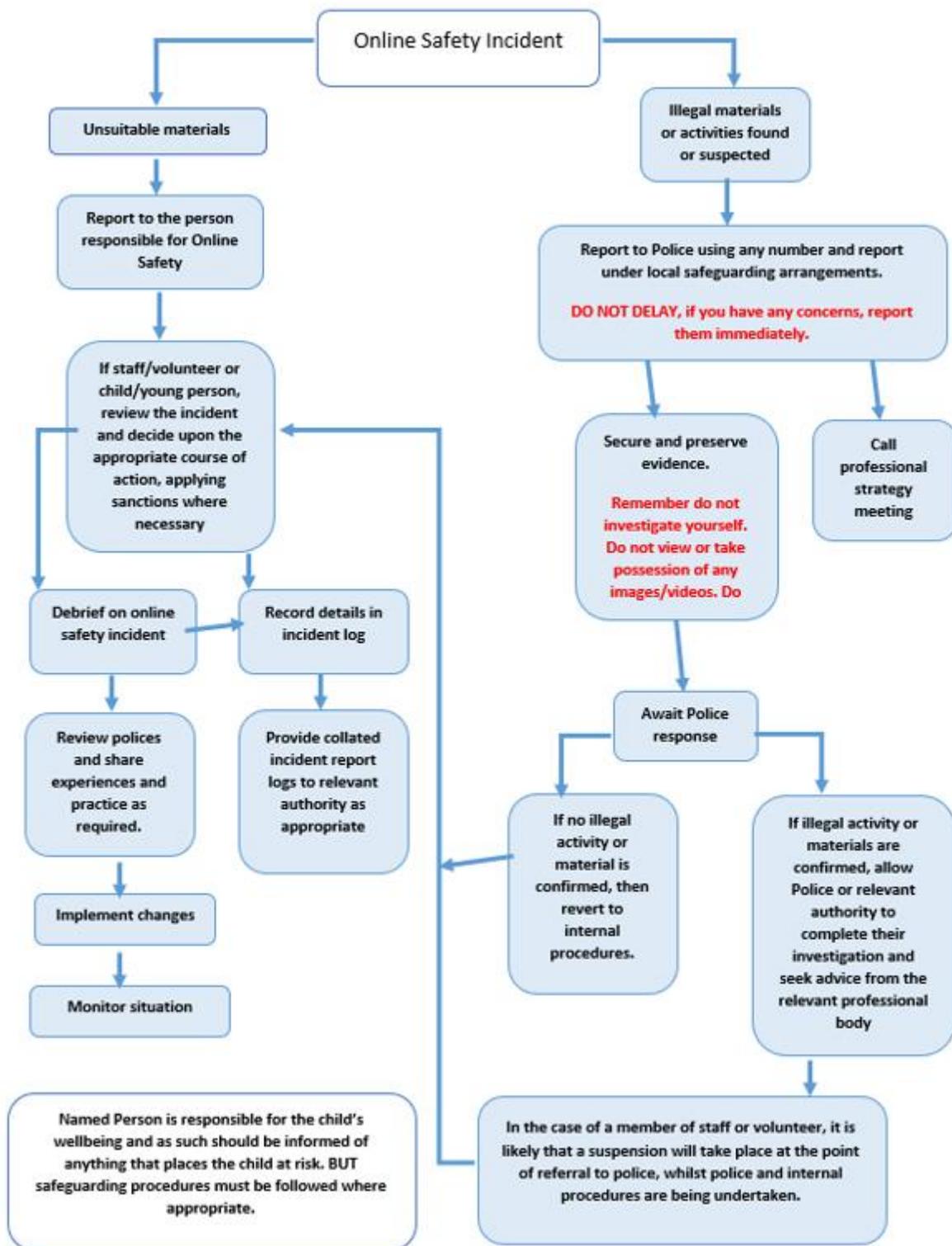
The **Governing Body, Headteacher** and **Online Safety Lead** review this policy in full on an **annual** basis and following any online safety incidents.

The school recognises that the online world is constantly changing; therefore, the Online Safety Lead and the headteacher conduct light-touch reviews of this policy throughout the year to evaluate its effectiveness.

The next scheduled review date for this policy is **November 2023**.

Any changes made to this policy are communicated to all members of the school community.

Appendix 1: Responding to incidents of misuse – flow chart



Appendix 2: Record of reviewing devices/internet sites (responding to incidents of misuse)

Device:

Date:

Reason for investigation:

Details of first reviewer

Name:

Position:

Signature:

Details of second reviewing person

Name:

Position:

Signature:

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

<i>Website(s) address/device</i>	<i>Reason for concern</i>

Conclusion and Action proposed or taken

Appendix 3:

Training Needs Audit Log

Group:

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

Appendix 4:

Appendix 5: 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/online-safety>

Childnet – <https://www.childnet.com>

Professionals Online Safety Helpline - <https://saferinternet.org.uk/professionals-online-safety-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 - <https://www.ceop.police.uk>

[ThinkUKnow](https://www.thinkuknow.co.uk/) - <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/>

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://hackinghate.eu/>

Scottish Anti-Bullying Service, Respectme - <https://respectme.org.uk/>

Scottish Government - Better relationships, better learning, better behaviour - <https://www.gov.scot/publications/developing-positive-whole-school-ethos-culture-relationships-learning-behaviour/>

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:

<https://www.childnet.com/what-we-do/our-projects/cyberbullying-guidance-and-practical-toolkit/>

[Childnet – Project deSHAME – Online Sexual Harrassment](#)

[UKSIC – Sexting Resources](#)

[Ditch the Label – Online Bullying Charity](#)

[Diana Award – Anti-Bullying Campaign](#)

Social Networking

UKSIC - [Safety Features on Social Networks](#)

[Children’s Commissioner, TES and Schillings – Young peoples’ rights on social media](#)

Curriculum

Purple Mash – access through <https://www.welearn365.com/>

SWGfL Evolve - <https://projectevolve.co.uk>

[UKCCIS – Education for a connected world framework](#)

Department for Education: Teaching Online Safety in Schools

Teach Today – <https://www.teachtoday.de/en/>

Data Protection

[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](#)

[UK Safer Internet Centre Professionals Online Safety Helpline](#)

Infrastructure/Technical Support/Cyber-security

[UKSIC – Appropriate Filtering and Monitoring](#)

[SWGfL Safety & Security Resources](#)

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](#)