Believing and Achieving Together to be the Best We Can Be

We aim to reflect God's love, " I have come that they may have life, and have it to the full."
John 10:10

This policy has been developed and will be implemented in accordance with the Christian vision and values of both schools.

SCHOOL ONLINE SAFETY POLICY

Policy dated 5th February 2018

Reviewed & Updated Autumn 2025

Reviewed and approved by the Lead Governors for Safeguarding, on behalf of the Governing Board on:

Next yearly review: Autumn 2026

Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of Feniton 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).
Feniton 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.

Development / Monitoring / Review of this Policy

This e-safety policy has been developed by a working group made up of:

- *senior leaders*
- *Designated safeguarding lead (DSL)*
- *Online Safety Lead (OSL)*
- *staff – including teachers/support staff/technical staff*
- *governors*
- *parents and carers*
- *community users*

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for Development / Monitoring / Review

This e-safety policy was approved by delegated authority to Safeguarding Lead Governor and presented at Full Governing Board	*29.03.2021*
The implementation of this e-safety policy will be monitored by the:	*Online Safety Lead, Safeguarding Lead Governor, Senior Leadership Team,*
Monitoring will take place at regular intervals:	*Once a year*
The Governors Sub Committee will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	*Once a year*
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be Spring 2025	Safeguarding Lead Governor
Should serious online safety incidents take place, the following external persons / agencies should be informed:	*DPO – DPG@devonmoorsfederation.devon.sch.uk* *LADO – 01392 384964* *MASH (Front Door) – 03451551071* *Police - 101* *Professional Online Safety Helpdesk - 03443814772*

The school will monitor the impact of the policy using:

- *Logs of reported incidents*
- *Surveys / questionnaires of:*
- *students / pupils*
- *parents / carers*
- *staff*

Roles and Responsibilities

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

Executive Headteacher / Head of School:

- The Executive Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
- The Executive Headteacher and Heads of School 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 Executive Headteacher and Heads of School are responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The Executive Headteacher and Heads of School 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 Executive Headteacher and Heads of School will receive regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead.
- The Executive Headteacher and Head of Schools will work with the responsible Governor, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.

Governors

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

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

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

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 Safeguarding Lead 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:

1. regular meetings with the Designated Safeguarding Lead
2. regularly receiving (collated and anonymised) reports of online safety incidents
3. checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
4. 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 DSL, and the IT service provider and involve the responsible governor) - in-line with the DfE Filtering and Monitoring Standards
5. reporting to relevant governors group/meeting
6. Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards

Designated Safety Lead (DSL) and Online Safety Lead (OSL):

Keeping Children Safe in Education states that:

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

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

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

The DSL will:

- hold the lead responsibility for online safety, within their safeguarding role.
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online.
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out (Exec Head responsibility).
- attend relevant governing body meetings/groups.
- report regularly to Executive Headteacher.
- 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)

- 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 Computeam, Devon County Council, Computing Technicians as required
- 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:
    1. content
    2. contact
    3. conduct
    4. commerce

Computing Team

Curriculum Leads will work with the DSL to develop a planned and coordinated online safety education programme through the use of Project EVOLVE.

This will be provided (amend/delete as relevant) through:

- Computing, PSHRE and wider curriculum programmes
- Assemblies
- Relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

Teaching and support staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/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 follow all relevant guidance and legislation including, for example, Keeping Children Safe in Education and UK GDPR regulations
- all digital communications with learners, parents and carers and others should be on a professional level and only carried out using official school systems and devices (where staff use AI, they should only use school-approved AI services for work purposes which have been evaluated to comply with organisational security and oversight requirements – CoPilot)
- they immediately report any suspected misuse or problem to DSL 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 video-conferencing, 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.
- they adhere to the school's technical security policy, with regard to the use of devices, systems and passwords and have an understanding of basic cybersecurity
- they have a general understanding of how the learners in their care use digital technologies out of school, in order to be aware of online safety issues that may develop from the use of those technologies
- they are aware of the benefits and risks of the use of Artificial Intelligence (AI) services in school, being transparent in how they use these services, prioritising human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans, fact-checked and critically evaluated.

IT Provider

The DfE Filtering and Monitoring Standards says:

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

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

"The IT service provider should have technical responsibility for:

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

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

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

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 local authority / MAT 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 Executive 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 systems are implemented and regularly updated as agreed in school policies.

Learners:

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- should know what to do if they or someone they know feels vulnerable when using online technology.
- should avoid plagiarism and uphold copyright regulations, taking care when using Artificial Intelligence (AI) services to protect the intellectual property of themselves and others and checking the accuracy of content accessed through AI services.

Parents / Carers

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

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

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

Community Users
Community users who access school systems/website/learning platform as part of the wider school provision will be expected to sign a community user AUA before being provided with access to school systems.

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

Professional Standards
There is an expectation that professional standards will be applied to online safety as in other aspects of school life i.e.

- there is a consistent emphasis on the central importance of literacy, numeracy, digital competence and digital resilience. Learners will be supported in gaining skills across all areas of the curriculum and every opportunity will be taken to extend learners' skills and competence

- there is a willingness to develop and apply new techniques to suit the purposes of intended learning in a structured and considered approach and to learn from the experience, while taking care to avoid risks that may be attached to the adoption of developing technologies e.g. Artificial Intelligence (AI) tools.

- Staff are able to reflect on their practice, individually and collectively, against agreed standards of effective practice and affirm and celebrate their successes

- 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.

- Where Generative AI is used to monitor staff communications, it will be balanced with respect for privacy and transparency about what is being monitored and why.

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

Acceptable use agreements
An Acceptable Use Agreement is a document that outlines a school's expectations on the responsible use of technology by its users. In most schools they are signed or acknowledged by their staff as part of their conditions of employment.

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,	**Any illegal activity for example:** • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	• 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					
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) N.B. Schools will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. The National Crime Agency has a remit to prevent learners becoming involved in cyber-crime and harness their activity in positive ways– further information here					X

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 and intellectual property (including through the use of AI services.)				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	

	Staff and other adults	**Learners**

Consideration should be given for the following activities when undertaken for non-educational purposes: Schools may wish to add further activities to this list.	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission
Online gaming	X						X	
Online shopping/commerce			X		X			
File sharing			X					X
Social media	X				X			
Entertainment streaming e.g. Netflix, Disney+	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				X			
Use of personal e-mail in school, or on school network/wi-fi			X		X X			
Use of school e-mail for personal e-mails	X				X			

X X

Use of AI services that have not been approved by the school								

When using communication technologies, the school considers the following as good practice:

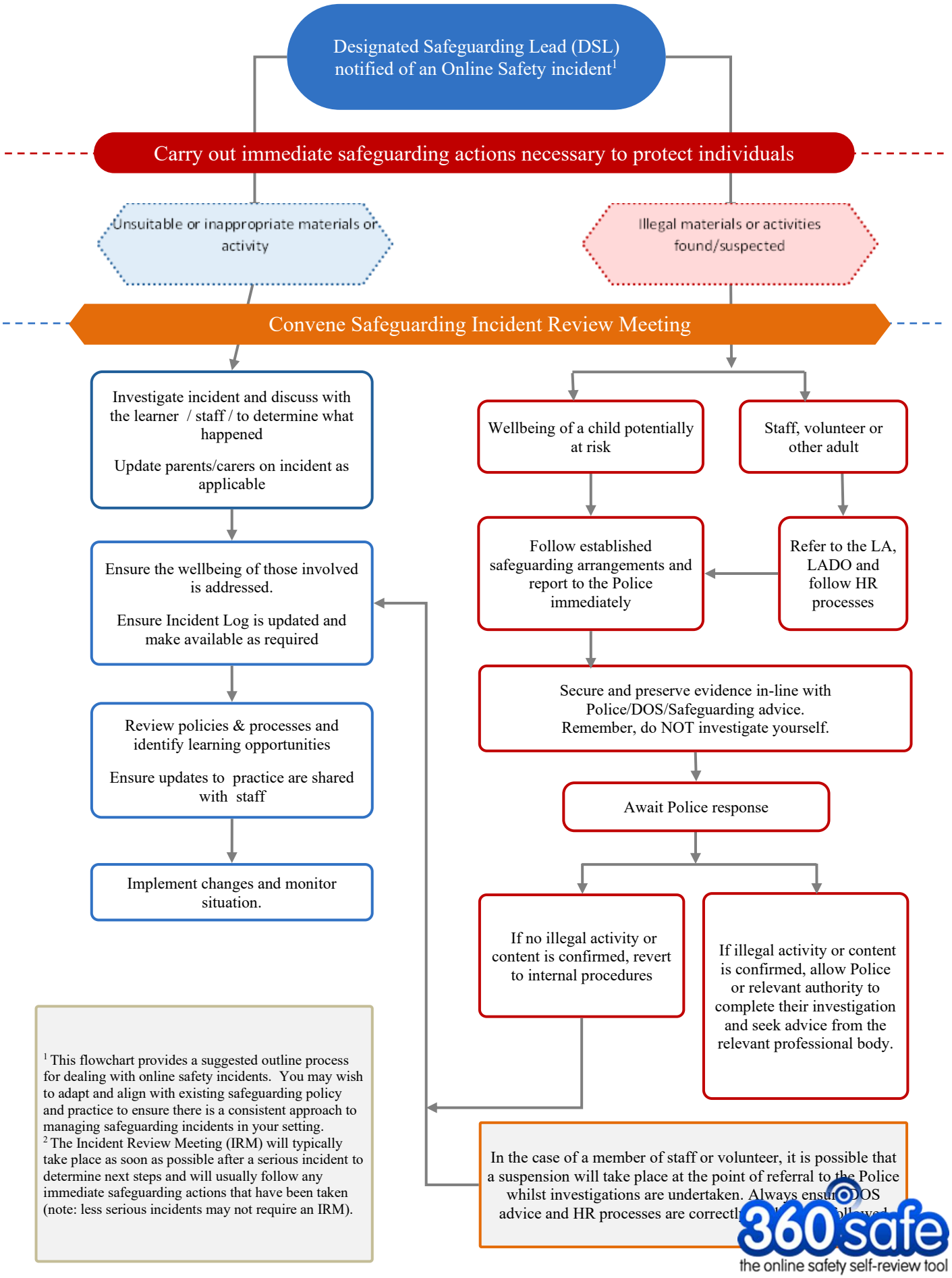
- when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school.
- any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. *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.

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 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 the incident must be escalated through the agreed school safeguarding procedures, this may include:

1. Non-consensual images
2. Self-generated images
3. Terrorism/extremism
4. Hate crime/ Abuse
5. Fraud and extortion
6. Harassment/stalking
7. Child Sexual Abuse Material (CSAM)
8. Child Sexual Exploitation Grooming
9. Extreme Pornography
10. Sale of illegal materials/substances
11. Cyber or hacking offences under the Computer Misuse Act
12. Copyright theft or piracy


Designated Safeguarding Lead (DSL) notified of an Online Safety incident[1]
Carry out immediate safeguarding actions necessary to protect individuals
Unsuitable or inappropriate materials or activity
Illegal materials or activities found/suspected
Convene Safeguarding Incident Review Meeting
Investigate incident and discuss with the learner / staff / to determine what happened
Update parents/carers on incident as applicable
Ensure the wellbeing of those involved is addressed.
Ensure Incident Log is updated and make available as required
Review policies & processes and identify learning opportunities
Ensure updates to practice are shared with staff
Implement changes and monitor situation.
Wellbeing of a child potentially at risk
Staff, volunteer or other adult
Follow established safeguarding arrangements and report to the Police immediately
Refer to the LA, LADO and follow HR processes
Secure and preserve evidence in-line with Police/DOS/Safeguarding advice. Remember, do NOT investigate yourself.
Await Police response
If no illegal activity or content is confirmed, revert to internal procedures
If illegal activity or content is confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body.
In the case of a member of staff or volunteer, it is possible that a suspension will take place at the point of referral to the Police whilst investigations are undertaken. Always ensure DOS advice and HR processes are correctly followed.
[1] This flowchart provides a suggested outline process for dealing with online safety incidents. You may wish to adapt and align with existing safeguarding policy and practice to ensure there is a consistent approach to managing safeguarding incidents in your setting.
[2] The Incident Review Meeting (IRM) will typically take place as soon as possible after a serious incident to determine next steps and will usually follow any immediate safeguarding actions that have been taken (note: less serious incidents may not require an IRM).
360safe
the online safety self-review tool

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.

Responding to Learner Actions

Incidents	Refer to class teacher/tutor	Refer to Head of School	Refer to EHT	Refer to Police/Social Work	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	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	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
Unauthorised downloading or uploading of files or use of file sharing.	X	X				X	X		X
Using proxy sites or other means to subvert the school's filtering system.	X	X	X			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	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	
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			X	X		X
Continued infringements of the above, following previous warnings or sanctions.	X	X	X	X		X	X		X

Responding to Staff Actions

Incidents	Refer to Head of School	Refer to Executive Headteacher	Refer to local authority/HR	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	X
Actions which breach data protection or network / cyber-security rules.	X	X	X	X	X		X	X
Deliberately accessing or trying to access offensive or pornographic material.	X	X	X	X			X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software.	X	X	X	X	X		X	X
Using proxy sites or other means to subvert the school's filtering system.	X	X	X	X	X		X	X
Unauthorised downloading or uploading of files or file sharing.	X	X				X		
Breaching copyright/ intellectual property or licensing regulations (including through the use of AI systems.)	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	X	X
Using personal e-mail/social networking/messaging to carry out digital communications	X	X			X	X		X

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

The use of Artificial Intelligence (AI) systems in School

As Generative Artificial Intelligence (gen AI) continues to advance and influence the world we live in, its role in education is also evolving. There are currently 3 key dimensions of AI use in schools: learner support, teacher support and school operations; ensuring all use is safe, ethical and responsible is essential. We realise that there are risks involved in the use of Gen AI services, but that these can be mitigated through our existing policies and procedures, amending these as necessary to address the risks. We will educate staff and learners about safe and ethical use of AI, preparing them for a future in which these technologies are likely to play an increasing role. The safeguarding of staff and learners will, as always, be at the forefront of our policy and practice.

The school acknowledges the potential benefits of the use of AI in an educational context - including enhancing learning and teaching, improving outcomes, improving administrative processes, reducing workload and preparing staff and learners for a future in which AI technology will be an integral part. Staff are encouraged to use AI based tools to support their work where appropriate, within the policy provided below and are required to be professionally responsible and accountable for this area of their work.
As per the October 2023 Department for Education policy paper Generative artificial intelligence (AI) in education - GOV.UK, staff must '*not allow or cause intellectual property*[1]*, including pupils' work, to be used to train generative AI models, without appropriate consent or exemption to copyright'.*
Parents or legal guardians have the right to withdraw their consent for the use of their child's intellectual property in conjunction with generative AI applications and programs.
To support this statement, the Federation will only approve AI applications that do not use data to train the machine learning model. Where new applications are requested as part of continuous review process, the reviewer will specifically seek privacy data to ensure that pupil intellectual property is protected. Where an application requested does use pupil data, the requestee must provide substantial evidence that this application has a clear teaching and learning purpose. Approvals will be made on a case-by-case basis, and specific consent from parents will be sought to cover each of these applications.

Transparency with stakeholders: pupils, parents, governors

In implementing AI in education, transparency with stakeholders - pupils, parents, and governors - is crucial. Otter Valley Federation will communicate with our community where, how and why we are using AI. Pupils must understand how AI impacts their learning, while parents need to know how it enhances education and safeguards privacy. Governors require detailed updates on AI strategies, educational impacts, and ethical compliance.
Communication of our implementation is identified within this policy, which is freely available on our Federation website.
Through the Relationships and Health Education Curriculum, pupils will be taught about artificial intelligence in an age-appropriate manner. Additionally, before pupils use AI in Federation schools, a separate Pupil AI policy will be developed.

[1] Pupils own the **intellectual property** (IP) rights to original content they create. Intellectual property can only be used to train AI if there is consent from the rights holder or an exemption to copyright applies. Education institutions must not allow or cause pupils' original work to be used to train generative AI models unless they have appropriate consent or exemption to copyright. Consent would need to be from the student if over 18, and from their **parent or legal guardian** if under 18.

Promote Ethical and Fair Use of AI:

Otter Valley Federation is committed to promoting the ethical and fair use of AI to support education colleagues and enhance the learning experience. By integrating AI responsibly, we aim to address issues such as bias and fairness, ensuring that all AI tools are used transparently and ethically.

Bias and Fairness in Artificial Intelligence.

With reference to Ofsted's April 2024 Policy Paper Ofsted's approach to artificial intelligence (AI) - GOV.UK, education providers must:

- Ensure they can identify and rectify bias or error.
- Only use AI solutions that are ethically appropriate – in particular, to consider bias relating to small groups and protected characteristics before using AI
- Monitor bias closely and correct problems where appropriate

Bias is inclination or prejudice for or against one person or group, especially in a way considered to be unfair. As AI is machine learning, it has therefore been pre-programmed with bias from the data it was trained with. Where staff are unsure of the data used to train the generative AI model, they must seek to monitor and address bias manually when re-drafting their AI exports.
All staff must ensure that the use of AI tools aligns with ethical standards in education, particularly regarding fairness, transparency, and inclusivity.

When staff use generative AI to create content for their role, they retain ownership of the created material. It is their responsibility to proofread and ensure the accuracy of the content, as well as to challenge and address any potential biases present in the data. This ensures that the use of AI aligns with the federation's commitment to ethical standards and fairness

Support Colleagues and Enhance Teaching Methods:

Otter Valley Federation aims to leverage the power of AI to support staff wellbeing by reducing workload. AI-powered tools can achieve this by offering a range of tools designed to significantly reduce the workload, thereby enhancing the efficiency and effectiveness of their roles, including teaching practice and administration.

Professional Responsibility

In the integration of AI tools to support colleagues, reduce workload and enhance teaching methods, it's crucial to emphasise the professional responsibility and oversight of all staff to manage and utilise these tools. While AI offers substantial benefits in terms of efficiency and personalisation, the ultimate responsibility for the educational process remains with the staff.

Approval and Accountability, Implementation:

To ensure a structured and responsible approach to AI implementation in the Federation, the Executive Headteacher and Heads of School will be assigned to oversee this integration. These leaders are responsible for guiding and supervising all aspects of AI adoption. Their roles include evaluating the educational value of proposed AI tools, ensuring compliance with legal and ethical standards, and aligning AI initiatives with the Federation's educational goals and policies.

Whitelist of Trust Approved AI Tools

Otter Valley Federation will build a comprehensive list of approved AI tools to ensure fairness and clarity in staff usage. These tools will be carefully selected based on the criteria outlined in this

policy, including data security, ethical considerations, and educational value. By providing a clear and vetted list, the federation aims to support staff in using AI responsibly and effectively, aligning with our commitment to transparency and ethical standards. Currently on the list:

- **CoPilot accessed through school Microsoft 365 account.**

Processes for sign off on the introduction of AI tools:

The introduction of AI tools at Otter Valley Federation follows a formalised approval process completed by our Data Protection Officer to ensure accountability and alignment with the Federation's educational objectives. This process includes: a proposal, including the purpose, benefits, costs, and potential risks associated with the AI tool and an impact assessment, focusing on educational outcomes and/or workload efficiency, data privacy, and ethical considerations.
All staff can submit a request in writing to the Executive Headteacher and Head of School for the introduction of a new AI tool.
The form will be sent directly to DPO for approval. Who will oversee AI implementation and will approve or decline proposals.

References

Generative artificial intelligence (AI) in education - GOV.UK
Data protection in schools - Generative artificial intelligence (AI) and data protection in schools - Guidance - GOV.UK
Generative AI in education: user research and technical report - GOV.UK
Research on public attitudes towards the use of AI in education - GOV.UK
Ofsted's approach to artificial intelligence (AI) - GOV.UK
Schools - NCSC.GOV.UK
AI Use in Assessments: Protecting the Integrity of Qualifications - JCQ Joint Council for Qualifications

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 the nationally agreed framework 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. PSHRE; Computing and the wider curriculum.
- 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.

- Learners should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information (including where the information is gained from Artificial Intelligence services)
- Learners should be taught to acknowledge the source of information used and to respect copyright / intellectual property when using material accessed on the internet and particularly through the use of Artificial Intelligence services
- 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.
- Staff 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/tools (including AI systems) 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 is relevant and up to date to ensure the quality of learning and outcomes.

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 canvas learner feedback and opinion.
- 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.

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, data protection and cyber- security 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 Designated Safeguarding 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/team meetings/INSET days
- the Designated Safeguarding Lead will provide advice/guidance/training to individuals as required.

Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group 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 or other relevant organisation (e.g., SWGfL)
- participation in school training / information sessions for staff or parents (this may include attendance at assemblies/lessons).

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
- Sharing good practice with other schools in clusters and or the local authority.

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.
- supporting community groups, e.g. early years settings, childminders, youth/sports/voluntary groups to enhance their online safety provision.

Technology

The DfE Filtering and Monitoring Standards states that ***"Your IT service provider may be a staff technician or an external service provider."*** If the school has an external technology provider, it is the responsibility of the school to ensure that the provider carries out all the online safety and security measures that would otherwise be the responsibility of the school. It is also important that the technology provider is fully aware of the school Online Safety Policy/acceptable use agreements and the school has a Data Processing Agreement in place with them. The school should also check their local authority/other relevant body policies on these technical and data protection issues if the service is not provided by the authority and will need to ensure that they have completed a Data Protection Impact Assessment (DPIA) for this contract.

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.

Filtering & Monitoring

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

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

The school filtering and monitoring provision is agreed by senior 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 DSL 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 Lead 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 Lead 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 e.g. using SWGfL Test Filtering.

Filtering

The DfE Technical Standards for Schools and Colleges states:

"Schools and colleges have a statutory responsibility to keep children and young people safe online as well as offline. Governing bodies and proprietors should make sure their school or college has appropriate filtering and monitoring systems in place, as detailed in the statutory guidance, Keeping children safe in education.

Filtering is preventative. It refers to solutions that protect users from accessing illegal, inappropriate and potentially harmful content online. It does this by identifying and blocking specific web links and web content in the form of text, images, audio and video.

These standards help school and college leaders, designated safeguarding leads and IT support understand how to work together to make sure they can effectively safeguard their students and staff."

- The Executive Headteacher and Safeguarding Lead Governor are responsible for ensuring these standards are met. Roles and responsibilities of staff and third parties, for example, in-house or third-party IT support are clearly defined.
- 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. These are acted upon in a timely manner, within clearly established procedures.
- There is a clear process in place to deal with, and log, requests/approvals for filtering changes.
- Filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.
- Devices that are provided by the school have school-based filtering applied irrespective of their location.
- The school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/learners, etc.)
- 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.

If necessary, the school will seek advice from, and report issues to, the SWGfL Report Harmful Content site.

Monitoring

The DfE Technical Standards for Schools and Colleges states:

"Monitoring is reactive. It refers to solutions that monitor what users are doing on devices and, in some cases, records this activity. Monitoring can be manual, for example, teachers viewing screens as they walk around a classroom. Technical monitoring solutions rely on software applied to a device that views a user's activity. Reports or alerts are generated based on illegal, inappropriate, or potentially harmful activities, including bullying. Monitoring solutions do not block users from seeing or doing anything."

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance.

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 Lead, all users are aware that the network (and devices) are monitored.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.
- The monitoring provision is reviewed at least once every academic year and updated in response to changes in technology and patterns of online safety incidents and behaviours. The review should be conducted by members of the senior leadership team, the designated safeguarding lead, and technical staff. It will also involve the responsible governor. The results of the review will be recorded and reported as relevant.
- Devices that are provided by the school have school-based monitoring applied irrespective of their location.
- monitoring enables alerts to be matched to users and devices.
- where AI –supported monitoring is used, the purpose and scope of this is clearly communicated

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)

Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended standards in the DfE Technical Standards for Schools and Colleges and others outlined in Devon County Council guidance:

- Responsibility for technical security resides with SLT who may delegate activities to identified roles.
- A documented access control model is in place, clearly defining access rights to school systems and devices. This is reviewed annually. All users (staff 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.
- Password policy and procedures are implemented. (consistent with guidance from the National Cyber Security Centre)
- All school networks, devices and system will be protected by secure passwords.
- 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 Executive 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/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. (See school personal data policy template in the appendix for further detail)
- 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.
- Systems are in place that prevent the unauthorised sharing of personal / sensitive data unless safely encrypted or otherwise secured. (See school personal data policy template in the appendix for further detail).
- Care will be taken when using Artificial Intelligence services to avoid the input of sensitive information, such as personal data, internal documents or strategic plans, into third-party AI

systems unless explicitly vetted for that purpose. Staff must always recognise and safeguard sensitive data.

- Dual-factor authentication is used for sensitive data or access outside of a trusted network
- Where AI services are used for technical security, their effectiveness is regularly reviewed, updated and monitored for vulnerabilities.
- Where AI services are used, the school will work with suppliers to understand how these services are trained and will regularly review flagged incidents to ensure equality for all users e.g. avoiding bias

Mobile technologies

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

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

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

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to those for safeguarding, behaviour, anti-bullying, acceptable use, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme.

In preparing a mobile technologies policy the school should consider possible issues and risks. These may include:

- security risks in allowing connections to your school network
- filtering of personal devices
- breakages and insurance
- access to devices for all learners
- avoiding potential classroom distraction
- network connection speeds, types of devices
- charging facilities
- total cost of ownership.

A range of mobile technology strategies is possible. However, these need to be thoroughly researched, risk assessed and aligned with existing policy prior to implementation.

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

Personal devices:

- Personal devices commissioned onto the school network are segregated effectively from school-owned systems Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device into the school lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in school.
- The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home.)
- The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues.
- The school recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Pass-codes or PINs should be set on personal devices to aid security.
- The school is not responsible for the day to day maintenance or upkeep of the users personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues.
- Where personal devices are brought to school, but their use is not permitted, appropriate, safe and secure storge should be made available.
- 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.
- 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.
- Staff owned devices should not be used for personal purposes during teaching sessions, unless in exceptional circumstances.
- Printing from personal devices will not be possible.

Social media

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

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

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

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

Personal use

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

Monitoring of public social media

- As part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school.
- 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.

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. Permission is not required for images taken solely for internal purposes.
- 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.

Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through (amend as necessary):

- Public-facing website
- Online newsletters

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.

The website includes an online reporting process for parents and the wider community to register issues and concerns to complement the internal reporting process.

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. The school may also wish to appoint a Data Manager and Systems Controllers to support the DPO.
- 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 (see Privacy Notice section in the appendix)
- 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 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.
- ensures that where AI services are used, data privacy is prioritised

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. (Be sure to select devices that can be protected in this way)
- 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. VPN access to the school network, or 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.

Cyber Security
The DfE Cyber security standards for schools and colleges explains:

"Cyber incidents and attacks have significant operational and financial impacts on schools and colleges. These incidents or attacks will often be an intentional and unauthorised attempt to access, change or damage data and digital technology. They could be made by a person, group, or organisation outside or inside the school or college and can lead to:

- ***safeguarding issues due to sensitive personal data being compromised***
- ***impact on student outcomes***
- ***a significant data breach***
- ***significant and lasting disruption, including the risk of repeated future cyber incidents and attacks, including school or college closure***
- ***financial loss***
- ***reputational damage"***

The 'Cyber-security in schools: questions for governing bodies and Trustees' guidance produced by the National Cyber Security Centre (NCSC) aims to support governing bodies' and management committees' understanding of their education settings' cyber security risks. The guidance includes eight questions to facilitate the cyber security conversation between the governing body and school leaders, with the governing body taking the lead.
The school may wish to consider the following statements, amending them in the light of their current cybersecurity policy, processes and procedures:

- the school has reviewed the DfE Cyber security standards for schools and colleges and is working toward meeting these standards.
- the school will conduct a cyber risk assessment annually and review each term
- the school, (in partnership with their technology support partner), has identified the most critical parts of the school's digital and technology services and sought assurance about their cyber security
- the school has an effective backup and restoration plan in place in the event of cyber attacks
- the school's governance and IT policies reflect the importance of good cyber security
- staff and Governors receive training on the common cyber security threats and incidents that schools experience
- the school's education programmes include cyber awareness for learners
- the school has a business continuity and incident management plan in place
- there are processes in place for the reporting of cyber incidents. All students and staff have a responsibility to report cyber risk or a potential incident or attack, understand how to do this feel safe and comfortable to do so.

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.