

# An amazing place to learn!

from nursery to Year 6!

'When I visited Captain Shaw's, it just lifted me off my feet and nourished my heart. The students, young as they are, are sharp, inquisitive, familiar with current issues, full of optimism and keen to engage and make a difference. Thanks for a truly visionary, encouraging and informative visit.'

Pushpanath Krishnamurthy  
International campaigner for Fairtrade and Climate Justice

'Oh my goodness! I am still buzzing from the amazing day we had with you and your wonderful school! I love the way you have designed your curriculum so that every lesson has a purpose and is part of an immersive experience, rather than just learning things in isolation.'

Gaye Holmes - Senior Presenter, Imoves



'The **conduct** of pupils at this school is **exemplary**. They demonstrate **warmth and kindness** towards each other. Pupils enjoy **respectful relationships** with the adults at school who care deeply for them.'


'Pupils respond well to the **high aspirations** that the school has of their achievement.'

'Pupils demonstrate a **high level of motivation** towards their learning. They **work exceptionally well together**. They are **well prepared** for each stage of their education.'

Ofsted 2023



## Online Safety Policy

Designated Safeguarding Lead (DSL)	Terentius Jackson
Online Safety Lead	As above
Remote Education Lead	As above
Online Safety / Safeguarding Link Governor	Helen Webber
Wellness Champion for Children	Louise May
Network Manager / other technical support	System IT / LA / CICT (Securly Filtering Solutions – from April 2025)
<b>Approved by</b>	
<b>Name:</b>	Terentius Jackson (to be approved by full governing board March 25)
<b>Position:</b>	Headteacher / DSL
<b>Signed:</b>	
<b>Date:</b>	March 2025
<b>Review date:</b>	February 2026 (or earlier)



Serving the Common Good:

Seek what is best for everyone, beginning with the last, the least, the lost, the most vulnerable and the most forgotten.

# Contents

Scope of the Online Safety Policy .....	2
Policy development, monitoring and review .....	2
Process for monitoring the impact of the Online Safety Policy .....	3
<b>Policy and leadership.....</b>	<b>3</b>
Responsibilities.....	3
Online Safety Group .....	7
Professional Standards .....	8
<b>Policy.....</b>	<b>8</b>
Online Safety Policy.....	8
Acceptable use .....	9
User actions .....	9
Reporting and responding .....	12
Online Safety Incident Flowchart.....	15
Responding to Learner Actions.....	16
Responding to Staff Actions .....	18
<b>The use of Artificial Intelligence (AI) systems in School .....</b>	<b>19</b>
Online Safety Education Programme.....	21
Contribution of Learners.....	22
Staff/volunteers .....	22
Governors .....	23
Families .....	23
Adults and Agencies .....	23
<b>Technology.....</b>	<b>24</b>
Filtering .....	24
Monitoring.....	25
Technical Security.....	25
Mobile technologies .....	27
Social media .....	27
Digital and video images.....	29
Online Publishing.....	30
Data Protection .....	30
Cyber Security (new January 2025) .....	32
<b>Outcomes .....</b>	<b>33</b>

## Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of Captain Shaw's C of E Primary School to safeguard members of our school community online in accordance with statutory guidance and best practice. Schools should be aware of the legislative framework under which this Online Safety Policy and guidance has been produced as outlined in the attached 'Legislation' Appendix.

**This Online Safety Policy applies to all members of the school community (including staff, learners, 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).**

Captain Shaw's C of E Primary School will deal with such incidents within this policy and associated behaviour policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

## Policy development, monitoring and review

This Online Safety Policy has been developed by the Headteacher / DSL & Online Safety lead and staff and reviewed by the Chair and Safeguarding link governor. This policy and associated codes of conduct, including acceptable user agreements have been issued to and are available on the website for:

- headteacher/senior leaders
- online safety lead
- 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.

## Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- logs of reported incidents on our safeguarding system
- monitoring of internet activity (including sites visited)
- internal monitoring data for network activity
- surveys/questionnaires of:
  - learners
  - parents and carers
  - staff.

## Policy and leadership

### 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<sup>1</sup> and groups within the school.

#### Headteacher and Safeguarding Leads

- 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<sup>2</sup>.
- The headteacher (DSL & online safety lead) is responsible for ensuring that the, technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- The Governors will receive regular monitoring reports from the Online Safety Lead (Headteacher).

#### Governors

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

---

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

“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”

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 Chair of Governors who will receive regular information about online safety incidents and monitoring reports. The Chair of Governors (also safeguarding link governor) will take on the role of Online Safety Governor to include:

- **weekly meetings with the Online Safety Lead**
- **regularly receiving (collated and anonymised) reports of online safety incidents**
- **checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)**
- **reporting to relevant governors group/meeting**
- membership of the school Online Safety Group
- occasional review of the filtering change control logs and the monitoring of filtering logs (where possible)

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

The Online Safety Lead will:

- lead the Online Safety Group
- take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns
- 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 staff 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, including reporting in our dedicated online safety subsections of our safeguarding system
- provide (or identify sources of) training and advice for staff/governors/parents/carers/learners
- liaise with (school/local authority/MAT/external provider) technical staff, pastoral staff and support staff (as relevant)
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and if possible, filtering and monitoring logs
- attend relevant governing body meetings/groups
- liaises with the local authority and associated external filtering arrangements for school

## Designated Safeguarding Lead (DSL)

The DfE guidance “Keeping Children Safe in Education” states:

“The designated safeguarding lead should take lead responsibility for safeguarding and child protection (**including online safety**). This should be explicit in the role holder’s job description.” ... Training should provide designated safeguarding leads with a good understanding of their own role, ... so they ... 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.”

The Designated Safeguarding Lead should be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:

- sharing of personal data <sup>3</sup>
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- online bullying.

### Curriculum

Staff will work with the Online Safety Lead to develop a planned and coordinated online safety education programme.

This will be provided through:

- A mapped, 'layers of safety' model including:
  - a discrete programme
  - PSHE and RHE programmes
  - assemblies and pastoral programmes
  - through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

### Teaching and support staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/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 on our safeguarding system and to the Headteacher/DSL for investigation/action, in line with the school safeguarding procedures
- 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
- 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

---

<sup>3</sup> See 'Personal data policy' in the Appendix.

- 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 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 e.g. children understanding they cover the screen and report to a member of staff immediately. Learners will also not have access to the URL bar (unless permitted by the member of staff). They will use 'Swiggle' search engine on both the laptops and iPads.
- where lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the [SWGfL Safe Remote Learning Resource](#)
- 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.

### Network manager/technical staff

The school has a technology service provided by an outside contractor, however, it is still the responsibility of the school to ensure that the provider carries out all the online safety measures that the school's obligations and responsibilities require. It is also important that the provider follows and implements school Online Safety Policy and procedures.

The technology 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 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/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 (see appendix 'Technical Security Policy template' for good practice).
- monitoring software/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 understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

## Parents and carers

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

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

- publishing the school Online Safety Policy on the school website
- providing them with a copy of the learners' acceptable use agreement
- publish information about appropriate use of social media relating to posts concerning the school
- seeking their permissions concerning digital images, cloud services etc (see parent/carer AUA in the appendix)
- parents'/carers' website, social media and information about national/local online safety campaigns and literature e.g. monthly online safety tips

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

- reinforcing the online safety messages provided to learners in school

## 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. (A community user's acceptable use agreement template can be found in the appendices).

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

## Online Safety Group

The Online Safety Group is the same as our safeguarding group and has the following members:

- Headteacher - Designated Safeguarding Lead / Online safety Lead
- EYFS Deputy Safeguarding Lead
- KS1 Deputy Safeguarding Lead
- Safeguarding governor
- Pupil Progress and welfare Governing board subcommittee (including parent/community representation)
- teacher and support staff members
- School council

Members will assist the Online Safety Lead with:

- the production/review/monitoring of the school Online Safety Policy/documents
- the production/review/monitoring of the school filtering and requests for filtering changes
- mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression and coverage
- reviewing network/filtering/monitoring/incident logs, where possible

- encouraging the contribution of learners to staff awareness, emerging trends and the school online safety provision
- consulting stakeholders – including staff/parents/carers about the online safety provision
- monitoring improvement actions identified through use of the 360-degree safe self-review tool.

## Professional Standards

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

## Policy

### Online Safety Policy

The DfE guidance “Keeping Children Safe in Education” states:

“**Online safety** and the school or college’s approach to it should be reflected in the child protection policy”

The school Online Safety Policy:

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

## Acceptable use

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

### Acceptable use agreements

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

- staff induction
- splash screens
- digital signage
- communication with parents/carers
- built into education sessions
- school website
- peer support.

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><b>Any illegal activity for example:</b></p> <ul style="list-style-type: none"> <li>• Child sexual abuse imagery*</li> <li>• Child sexual abuse/exploitation/grooming</li> <li>• Terrorism</li> <li>• Encouraging or assisting suicide</li> <li>• Offences relating to sexual images i.e., revenge and extreme pornography</li> <li>• Incitement to and threats of violence</li> <li>• Hate crime</li> <li>• Public order offences - harassment and stalking</li> <li>• Drug-related offences</li> <li>• Weapons / firearms offences</li> <li>• Fraud and financial crime including money laundering</li> </ul> <p>N.B. Schools should refer to guidance about dealing with self-generated images/sexting – <a href="#">UKSIC Responding to and managing sexting incidents</a> and <a href="#">UKCIS – Sexting in schools and colleges</a></p>					X
Users shall not undertake activities that might be classed as cyber-crime under	<ul style="list-style-type: none"> <li>• 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)</li> <li>• Gaining unauthorised access to school networks, data and files, through the use of computers/devices</li> </ul>					X

User actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
<p>the Computer Misuse Act (1990)</p> <ul style="list-style-type: none"> <li>• Creating or propagating computer viruses or other harmful files</li> <li>• Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords)</li> <li>• Disable/Impair/Disrupt network functionality through the use of computers/devices</li> <li>• Using penetration testing equipment (without relevant permission)</li> </ul> <p>N.B. Under Cyber-Prevent agenda the NCA has a remit to prevent learners becoming involved in cyber-crime and harness their activity in positive ways – info <a href="#">here</a></p>					
<p>Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:</p>	<p>Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)</p> <p>Promotion of any kind of discrimination</p> <p>Using school systems to run a private business</p> <p>Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school</p> <p>Infringing copyright</p> <p>Unfair usage (downloading/uploading large files that hinders others in their use of the internet)</p> <p>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</p>			<p>X</p> <p>X</p> <p>X</p> <p>X</p> <p>X</p> <p>X</p>	

Consideration should be given for the following activities when undertaken for <b>non-educational</b> purposes:  Schools may wish to add further activities to this list.	Staff and other adults				Learners			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission/awareness
Online gaming	X				X			
Online shopping/commerce			X		X			
File sharing				X				X
Social media			X		X			
Messaging/chat			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 (non-contact time only)		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			
---	---	--	--	--	--	---	--	--	--

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

- **any digital communication between staff and learners or parents/carers (e-mail, Parent messenger platform) 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.

## Reporting and responding

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

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

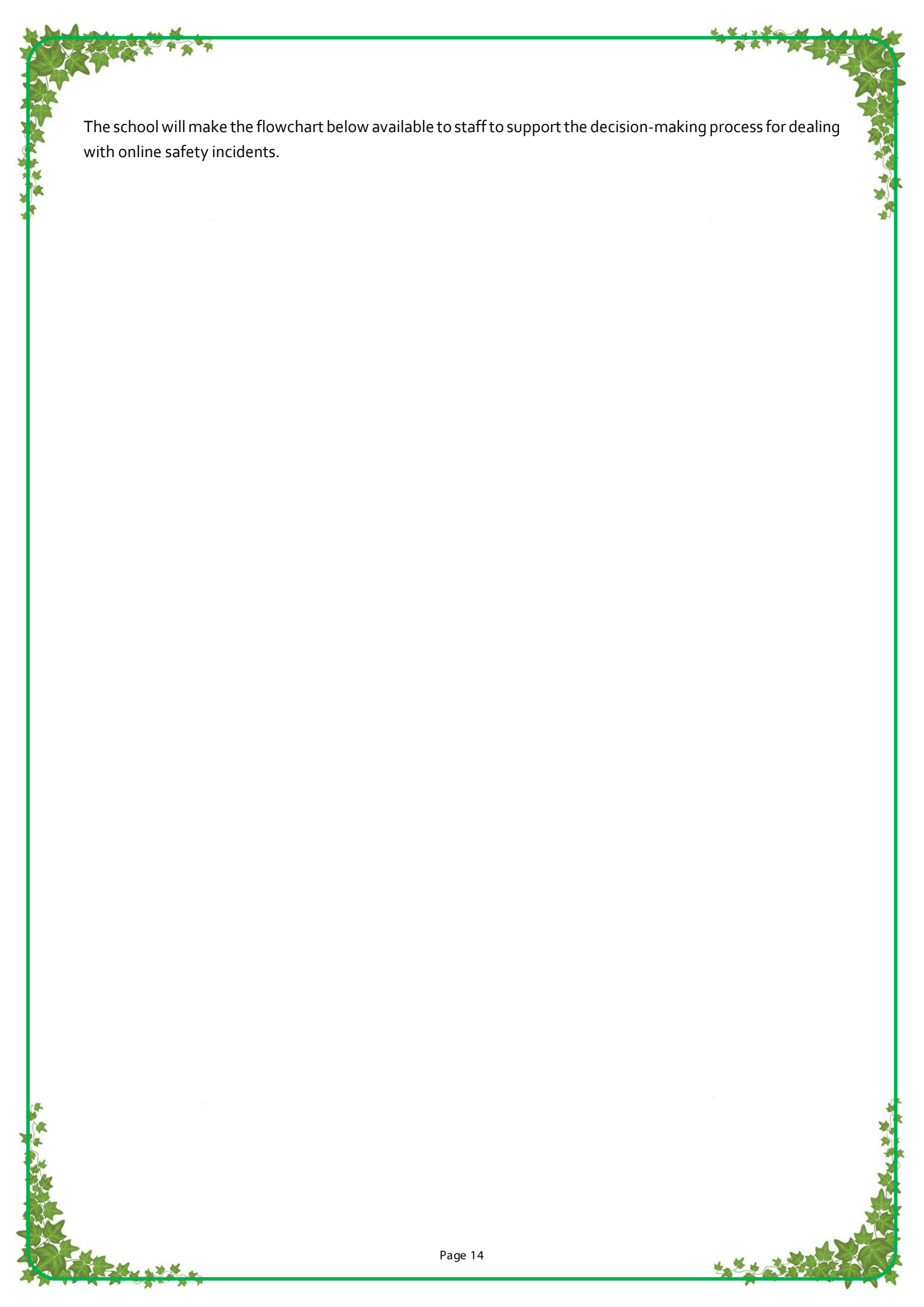
- *routine record-keeping and analysis of sexual harassment and sexual violence, including online, to identify patterns and intervene early to prevent abuse”*

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:

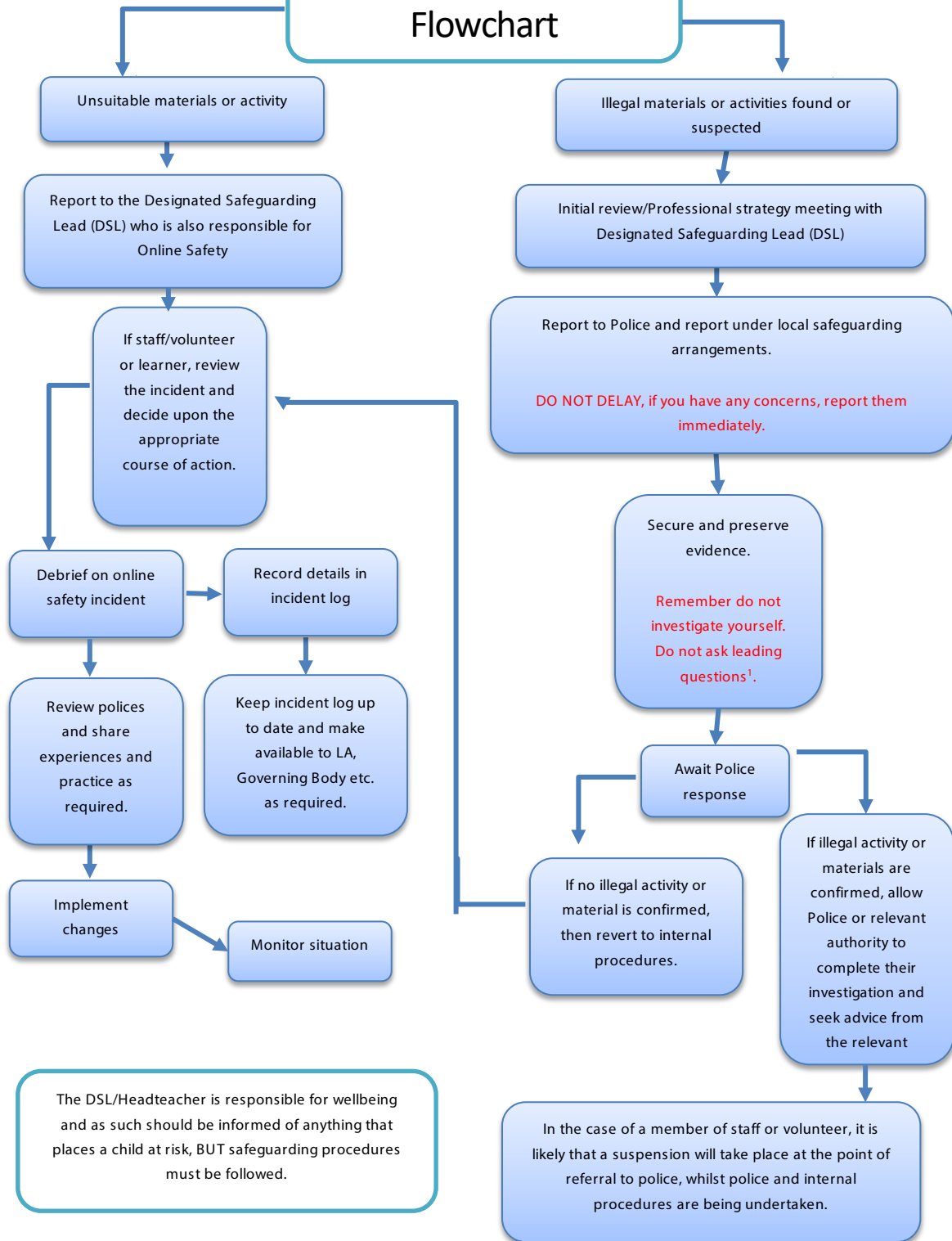
- **there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.**
- **all members of the school community will be made 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 and the local authority designated officer (see child protection and safeguarding policy and procedures).
- where there is no suspected illegal activity, devices may be checked using the following procedures:
  - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
  - conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
  - ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
  - record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form
  - once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - internal response or discipline procedures
    - involvement by local authority and Cumbria filtering service
    - police involvement and/or action
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident e.g., from our Child welfare Champion
- incidents should be logged on our safeguarding system immediately or as soon as practicably possible (within 24 hours)
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; [Professionals Online Safety Helpline](#); [Reporting Harmful Content](#); [CEOP](#).
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant)
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
  - the Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with
  - staff, through regular briefings
  - learners, through assemblies/lessons
  - parents/carers, through newsletters, school social media, website
  - governors, through regular safeguarding updates
  - local authority/external agencies, as relevant (The Ofsted Review into Sexual Abuse in Schools and Colleges suggested “working closely with Local Safeguarding Partnerships in the area where the school or college is located so they are aware of the range of support available to children and young people who are victims or who perpetrate harmful sexual behaviour”)

A decorative border of green ivy leaves and vines frames the page, starting from the top corners and extending down the sides.

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

# Online Safety Incident Flowchart



## 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	Refer to Headteacher	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		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
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature		X			X	X		X
Unauthorised downloading or uploading of files or use of file sharing.		X					X	
Using proxy sites or other means to subvert the school's filtering system.		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						
Unauthorised use of digital devices (including taking images)		X			X		X	
Unauthorised use of online services		X			X		X	
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.		X			X		X	
Continued infringements of the above, following previous warnings or sanctions.					X	X		X

# Responding to Staff Actions

Incidents	Refer to 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
Deliberate actions to breach data protection or network security rules.	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		
Unauthorised downloading or uploading of files or file sharing	X				X		
Breaching copyright or licensing regulations.	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
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature	X	X					X
Using personal e-mail/social networking/messaging to carry out digital communications with learners and parents/carers	X				X		

Inappropriate personal use of the digital technologies e.g. social media / personal e-mail	X				X		
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner	X				X		
Actions which could compromise the staff member's professional standing	X				X		
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.	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

## 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.

### Policy Statements

- 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 frameworks provided below and are required to be professionally responsible and accountable for this area of their work.
- **We will comply with all relevant legislation and guidance, with reference to guidance contained in Keeping Children Safe in Education and UK GDPR**

- We will provide relevant training for staff and governors in the advantages, use of and potential risks of AI. We will support staff in identifying training and development needs to enable relevant opportunities.
- We will seek to embed learning about AI as appropriate in our curriculum offer, including supporting learners to understand how gen AI works, its potential benefits, risks, and ethical and social impacts. The school recognises the importance of equipping learners with the knowledge, skills and strategies to engage responsibly with AI tools..
- As set out in the staff acceptable use agreement, staff will be supported to use AI tools responsibly, ensuring the protection of both personal and sensitive data. Staff should only input anonymised data to avoid the exposure of personally identifiable or sensitive information.
- Staff will always ensure AI tools used comply with UK GDPR and other data protection regulations. They must verify that tools meet data security standards before using them for work related to the school.
- Only those AI technologies approved by the school may be used. Staff should always use school-provided AI accounts for work purposes. These accounts are configured to comply with organisational security and oversight requirements, reducing the risk of data breaches.
- We will protect sensitive information. Staff must not input sensitive information, such as internal documents or strategic plans, into third-party AI tools unless explicitly vetted for that purpose. They must always recognise and safeguard sensitive data.
- The school will ensure that when AI is used, it will not infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.
- AI incidents must be reported promptly. Staff must report any incidents involving AI misuse, data breaches, or inappropriate outputs immediately to the relevant internal teams. Quick reporting helps mitigate risks and facilitates a prompt response.
- The school will audit all AI systems in use and assess their potential impact on staff, learners and the school's systems and procedures, creating an AI inventory listing all tools in use, their purpose and potential risks. [\(Risk assessment matrices are attached as an appendix\)](#)
- We are aware of the potential risk for discrimination and bias in the outputs from AI tools and have in place interventions and protocols to deal with any issues that may arise. When procuring and implementing AI systems, we will follow due care and diligence to prioritise fairness and safety.
- The school will support parents and carers in their understanding of the use of AI in the school
- Maintain Transparency in AI-Generated Content. Staff should ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance. Clearly marking AI-generated content helps build trust and ensures that others are informed when AI has been used in communications or documents.
- We will prioritise human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans and critically evaluate AI-generated outputs. They must ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing. This is especially important for external communication to avoid spreading misinformation.

- Recourse for improper use and disciplinary procedures. Improper use of AI tools, including breaches of data protection standards, misuse of sensitive information, or failure to adhere to this agreement, will be subject to disciplinary action as defined in Staff Disciplinary Policy.

## Online Safety Education Programme

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

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

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

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

- **A planned online safety curriculum for all year groups matched against a nationally agreed framework e.g. Education for a Connected Work Framework by UKCIS/DCMS and 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. PSHE; RHE; Digital Literacy; when researching in e.g. History.**
- **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 helped to understand the need for the learner 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 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 e.g. use of 'Swiggle' search engine dedicated to learner based websites.
- where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit

- it is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need
- **the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.**

## Contribution of Learners

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

- mechanisms to canvass learner feedback and opinion e.g. in lessons or through school council
- the Online Safety Group has learner representation through school council
- 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

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

"All staff should receive appropriate safeguarding and child protection training (**including online safety**) at induction. The training should be **regularly updated**. In addition, all staff should receive safeguarding and child protection (**including online safety**) updates (for example, via email, e-bulletins, and staff meetings), as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively."

"Governing bodies and proprietors should ensure... that safeguarding training for staff, **including online safety** training, is integrated, aligned and considered as part of the whole school or college safeguarding approach and wider staff training and curriculum planning."

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

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

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

## 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 (through our parent messaging system and website)
- regular opportunities for engagement with parents/carers on online safety issues through awareness workshops / parent/carer evenings
- 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.
- high profile events / campaigns e.g. Safer Internet Day
- reference to the relevant web sites/publications, e.g. SWGfL; [www.saferinternet.org.uk/](http://www.saferinternet.org.uk/); [www.childnet.com/parents-and-carers](http://www.childnet.com/parents-and-carers) (see Appendix for further links/resources).
- Sharing good practice with other schools in clusters and or the local authority

## 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*
- *the school will provide 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 e.g. supporting these groups with an online safety review using 360 Groups or 360 Early Years.*

## Technology

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

- the school filtering policies are agreed by the LA and technical staff and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours. The school will ensure technical staff inform the school of compliance at least annually
- 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 (see Appendix for more details).
- *the school has (if possible) 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](#)*
- filtering logs are regularly reviewed and alert the school to breaches of the filtering policy, which are then acted upon.
- *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 e.g. Apple management software*

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

# Monitoring

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

"It is essential that governing bodies and proprietors ensure that appropriate filters 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 filters 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 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. The DSL is 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/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 the appropriate blend of strategies strategy 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
- *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) – Securly Filtering Services / Cumbria ISP*

# 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 Online Safety Group
- 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 System IT 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, with System IT
- passwords should be long.
- 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. *Password complexity for younger learners may be reduced (for example 6 character maximum) and should not include special characters. Where external systems have different password requirements the use of random words or sentences should be encouraged*
- password requirements for learners at Key Stage 2 and above should increase as learners progress through school
- The 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. Learners will report to staff and staff will report to the Headteacher
- appropriate security measures are in place (managed by System IT) 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.
- an agreed policy is in place for the provision of temporary access of 'guests', (e.g., trainee teachers, supply teachers, visitors) onto the school systems. Access will only be permitted once an acceptable use agreement has been understood and signed
- an agreed policy is in place regarding the extent of personal use that staff are allowed on school devices that may be used out of school. These terms are detailed in the tables in this policy. Other members of a member of staff's family must not use school devices at home
- an agreed policy is in place that allows staff to/forbids staff from downloading executable files and installing programmes on school devices. If this is required, the Headteacher will submit a specific request to System IT, who will either install on our behalf or present a temporary administrator password to the Headteacher
- an agreed policy is in place regarding the use of removable media (e.g., memory sticks/CDs/DVDs) by users on school devices. Any memory sticks used for/in school must have been virus checked by the school / technical provider and must not contain any sensitive data
- systems are in place that prevent the unauthorised sharing of personal data unless safely encrypted or otherwise secured. (See school personal data policy template in the appendix for further detail)

## 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.*

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

The school allows:

	School devices			Personal devices		
	School owned for individual use	School owned for multiple users	Authorised device <sup>4</sup>	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	No	Yes	Yes
Full network access	Yes	Yes	Yes	No	No	No
Internet only				No	Yes*	Yes*
No network access						

\*In line with online safety, behaviour, code of conduct policies and signed acceptable use agreements

## Social media

The school uses the official website and a ‘closed’ parent communication system (GDPR compliant) where access is only permitted through invite. A parent/carer must have a child in the school. Data is not available to the general public.

<sup>4</sup> Authorised device – purchased by the learner/family through a school-organised scheme, e.g. for SEND. This device may be given full access to the network as if it were owned by the school.

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 but this must be during non-contact time with learners e.g. break times, lunch or PPA.

### 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.

If the school uses social media for professional purposes, it 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 e.g. the staff (school owned) iPads. 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 is 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. *These permissions can be found on the school's MIS (written permission is not required if photographs are for the school's internal use only)***
- **parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy**
- **images will be securely stored in line with the school retention policy**
- learners' work can only be published with the permission of the learner and parents/carers.

## Online Publishing

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

- Public-facing website
- 'Closed' Social media (parents/carers only have access)
- Official work email

The school website is managed/hosted by 'Primarysite'. 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.

## Data Protection

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

The school:

- **has a Data Protection Policy.**
- **implements the data protection principles and can demonstrate that it does so**
- **has paid the appropriate fee to the Information Commissioner's Office (ICO)**
- **has appointed an appropriate Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest.**
- **has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it**

- the Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed
- has an 'information asset register' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed
- will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school 'retention schedule' supports this
- data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- provides staff, parents, volunteers, teenagers, and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice (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

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

- data will be encrypted, and password protected.
- device will be password protected.
- device will be protected by up-to-date endpoint (anti-virus) software

- data will be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school
- only use encrypted data storage for personal data
- will not transfer any school personal data to personal devices. (staff are able to work from home using VPN access to the school network, using a work laptop)
- 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.

The Personal Data Advice and Guidance in the appendix (B2) provides more detailed information on the school’s responsibilities and on good practice.

## Cyber Security (new January 2025)

[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.