Online Safety Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents and guardians, visitors and community users) who have access to, and are users of, the school digital systems, both in and out of school. It also applies to the use of personal digital technology devises on the school site.

Authorised by the Governing Body: Yes Date: 4-11-25	
Produced by: Deputy Head (Pastoral Care and Safeguarding) and Head of Digital Learning 1-9-25	
Date Disseminated to the Staff via the intranet: 1-9-25	
Date of Review: 1-9-26	
Signed: James Pitt, Chair of Governors	

Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of Packwood Haugh 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, pupils, governors, volunteers, parents and guardians, visitors) 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).

Packwood Haugh 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.

Policy Development, Monitoring and Review

This Online Safety Policy has been developed by the
- *Head*
- *Designated safeguarding lead (DSL)*
- *Online Safety Lead (OSL)*
- *staff – including teachers/support staff/technical staff*

It will be monitored and reviewed by the Online Safety Group.

Schedule for Development, Monitoring and Reviews

This Online Safety Policy is to be approved by the *school governing body on:*	September 2025
The implementation of this Online Safety Policy will be monitored by:	DSL/OSL, Head of Digital Learning & SLT
Monitoring will take place at regular intervals:	Once a year - September
The *governing body* will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Three times a year as part of the Safeguarding Audit/Report to Governors.
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	September (or sooner if required by legislation changes)
Should serious online safety incidents take place, the following external persons/agencies should be informed:	LADO, Police, Governors

Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:
- logs of reported incidents
- Filtering and monitoring logs
- internal monitoring data for network activity
- surveys/questionnaires of:
  - pupils
  - parents and guardians
  - 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 and groups within the school.

The Head and senior Leaders

- The Head 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 Head and Deputy Head (Pastoral Care and Safeguarding) 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 Head is responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The Head 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 Head will receive regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead.
- The Head will work with the responsible Governor, the Designated Safeguarding Lead (DSL) and IT service providers in all aspects of filtering and monitoring.

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy and will refer to the UK Council for Internet Safety questions booklet.
This review will be carried out by the Prep School Committee whose members will receive regular information about online safety incidents and monitoring reports. A member of the governing body will take on the role of Online Safety Governor to include:

- regular meetings with the Designated Safeguarding Lead / 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)
- 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 involve the responsible governor)
- reporting to relevant *governors group/meeting*
- Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the
- *membership of the school Online Safety Group*

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

Designated Safeguarding Lead (DSL)

The DSL will:

- hold the lead responsibility for online safety, within their safeguarding role.

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

Online Safety Lead

The Online Safety Lead will:

- lead the Online Safety Group
- 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 (Head of Digital Learning)
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated (Head of Digital Learning)
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- provide (or identify sources of) training and advice for staff/governors/parents/carers/learners
- liaise with (school) technical staff, pastoral staff and support staff (as relevant)
- receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education:
  - o content
  - o contact
  - o conduct
  - o commerce

Curriculum Leads

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

This will be provided through:
- a discrete programme
- PHSE and RSE 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 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
- they immediately report any suspected misuse or problem to Sue Rigby 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 judgements, particularly those affecting people, are made by humans, fact-checked and critically evaluated.

Pupils

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy (this includes personal devices – where allowed)
- 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.
- In line with government guidance (2025), do not use AI in school, due to the age restriction set by AI tools. To this end, Copilot is disabled for all pupils.
- 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 Guardians

The school will take every opportunity to help parents and Guardians 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
- 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)*

<u>Online Safety Group</u>

The Online Safety Group has the following members:

- Designated Safeguarding Lead
- Online Safety Lead
- senior leaders
- online safety governor
- technical staff
- teacher and support staff members
- learners
- Parents and Guardians

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

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

Terms of Reference for the Online Safety Group terms can be found in the appendices.

Policy

The school Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world
- describes how the school will help prepare learners to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related acceptable use agreements
- is made available to staff at induction and through normal communication channels (in the staff handbook on the school's intranet and in hard copy in the school staff room).
- 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 and handbook
- posters/notices around where technology is used
- 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:	Any illegal activity for example: • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering					X

	• When dealing with self-generated images/sexting we will refer to 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) Refer to Cyber Choices - National Crime Agency for support for pupils/staff/parents					X
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)			X	X	
	Promotion of any kind of discrimination				X	
	Using school systems to run a private business				X	
	Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by the school				X	
	Infringing copyright				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Infringing copyright and intellectual property (including through the use of AI services)				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	

Consideration should be given for the following activities when undertaken for non-educational purposes: Schools may wish to add further activities to this list.	Staff and other adults				Pupils			
	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			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		x						x
Mobile phones may be brought to school		x						X (overseas pupils)
Use of mobile phones for learning at school				x				x
Use of mobile phones in social time at school								
Taking photos on mobile phones/cameras that are a work device		x						x
Use of other personal devices, e.g. tablets, gaming devices		x			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 (to email parents /guardians)		
Use of AI services that have not been approved by the school					X *AI is disabled*			

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

- when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school.
- any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. *Personal e-mail addresses, text messaging or social media must not be used for these communications.*
- staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community
- users should immediately report to a nominated person – in accordance with the school policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- *relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school e-mail addresses should be used to identify members of staff and learners.*
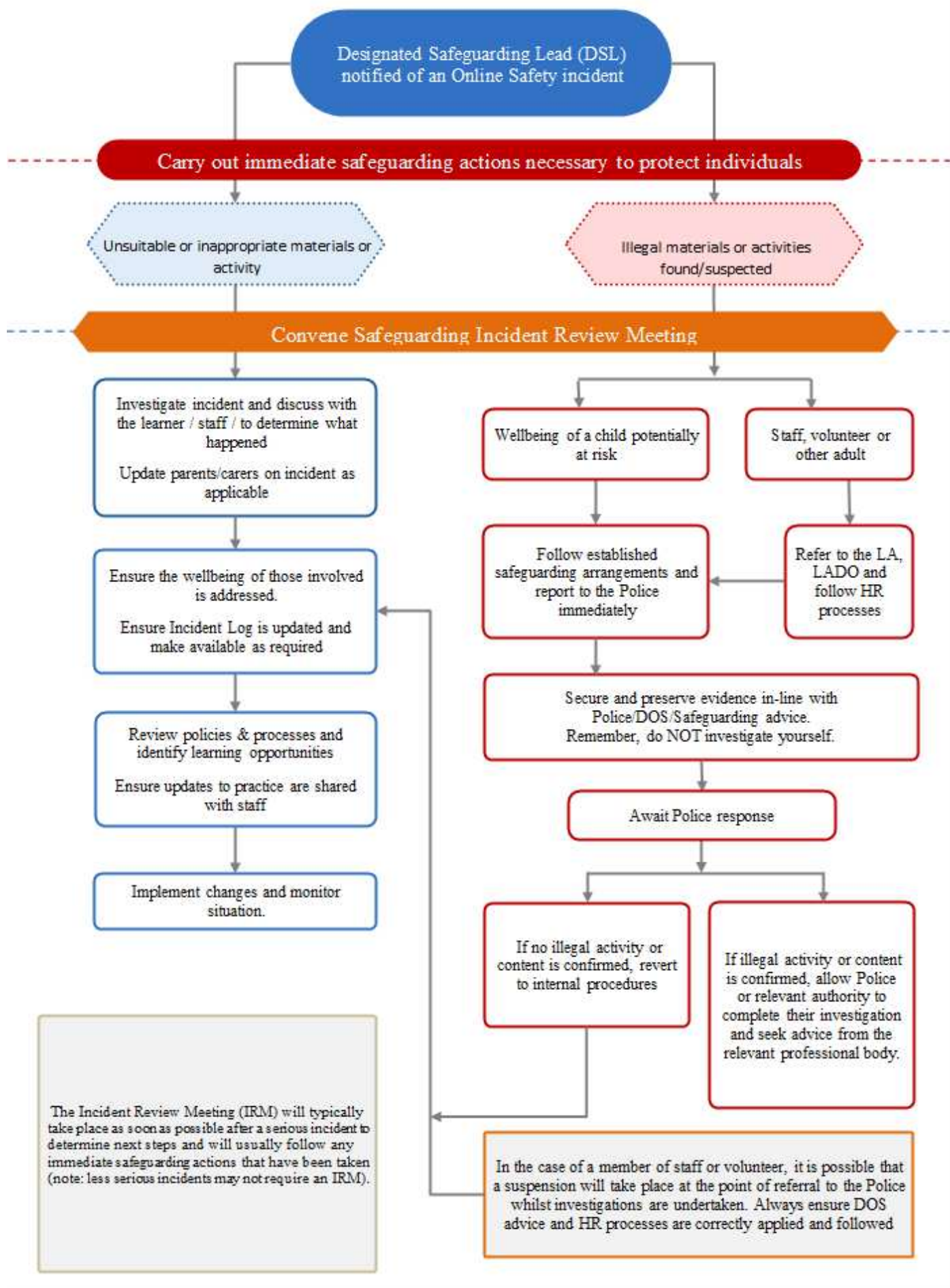
Reporting and Responding

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 dealing with allegations policies.
- all members of the school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm (see flowchart and user actions chart in the appendix), the incident must be escalated through the agreed school safeguarding procedures. This may include
    - o Non-consensual images
    - o Self-generated images
    - o Terrorism/extremism
    - o Hate crime/ Abuse
    - o Fraud and extortion
    - o Harassment/stalking
    - o Child Sexual Abuse Material (CSAM)
    - o Child Sexual Exploitation Grooming
    - o Extreme Pornography
    - o Sale of illegal materials/substances
    - o Cyber or hacking offences under the Computer Misuse Act
    - o Copyright theft or piracy
- any concern about staff misuse will be reported to the Head, unless the concern involves the Head, in which case the complaint is referred to the Chair of Governors and the local authority
- where AI is used to support monitoring and incident reporting, human oversight is maintained to interpret nuances and context that AI might miss
- 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:
    - o internal response or discipline procedures
    - o involvement by local authority / MAT (as relevant)
    - o police involvement and/or action
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents should be logged using the incident reporting log in the appendices and given to the DSL

- 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*
  - *pupils, through assemblies/lessons*
  - *parents/guardians, through newsletters, school social media, website*
  - *governors, through regular safeguarding updates*
  - *local authority/external agencies*

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

Designated Safeguarding Lead (DSL) notified of an Online Safety incident

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.

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).

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 applied and followed

Responding to pupil actions

Incidents	Refer to class teacher/tutor	Refer to Deputy Head	Refer to Head	Refer to Police/Social Work	Refer to local authority technical support for advice/action	Inform parents/guardians	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 above on unsuitable/inappropriate activities).			X	X		X			
Attempting to access or accessing the school network, using another user's account (staff or learner) or allowing others to access school network by sharing username and passwords	X					X		X	
Corrupting or destroying the data of other users.	X					X			X
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature	X					X			X
Unauthorised downloading or uploading of files or use of file sharing.	X					X		X	
Using proxy sites or other means to subvert the school's filtering system.	X	X				X		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
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.	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
Continued infringements of the above, following previous warnings or sanctions.			X			X	X		X

Responding to staff actions

Incidents	Refer to line manager/Deputy Head	Refer to Head	Refer to local authority/MAT/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 above on unsuitable / inappropriate activities)		X	X	X				
Actions which breach data protection or network/cyber-security rules.		X				X		
Deliberate actions to breach data protection or network security rules.		X				X		
Deliberately accessing or trying to access offensive or pornographic material		X						X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X		X				X
Using proxy sites or other means to subvert the school's filtering system.		X						X
Unauthorised downloading or uploading of files or file sharing	X					X		
Breaching copyright/ intellectual property or licensing regulations (including through the use of AI systems)	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
Using personal e-mail/social networking/messaging to carry out digital communications with learners and parents/carers	X							
Inappropriate personal use of the digital technologies e.g. social media / personal e-mail	X							
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner	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							
Continued infringements of the above, following previous warnings or sanctions.		X						X

Use of Artificial Intelligence (AI) 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.

With regard to government guidance (2025), pupils do not have access to AI tools, and as such Copilot has been disabled for all pupils. This is due to Microsoft's age limit of 13.

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.

- AI tools may be used to assist teachers in the assessment of learners' work, identification of areas for improvement and the provision of feedback. Teachers may also support learners to gain feedback on their own work using AI.
- 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'."

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

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways. A planned online safety curriculum for all year groups matched against a nationally agreed framework, the 'SWGfL Project Evolve', and regularly taught in a variety of contexts.

- Lessons are matched to need; are age-related and build on prior learning
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- Learner need and progress are addressed through effective planning and assessment
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Literacy etc
- it incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- the programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- 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. Lessons and further resources are available on the CyberChoices site.
- staff should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites / tools (including AI systems) the learners 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 pupils

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

- *mechanisms to canvass learner feedback and opinion.*
- *appointment of digital leaders/anti-bullying ambassadors/peer mentors*
- *the Online Safety Group has learner representation*
- *learners contribute to the online safety education programme e.g. peer education, digital leaders leading lessons for younger learners, online safety campaigns*
- *learners designing/updating acceptable use agreements*
- *contributing to online safety events with the wider school community e.g. videos; leaflets/posters; digital leaders*

Contribution of 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 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
- 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 Online Safety Lead and Designated Safeguarding Lead (or other nominated person) 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 Designated Safeguarding Lead/Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.

Contribution of 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

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

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

Contribution of 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 producing information videos and leaflets.
- letters, newsletters
- high profile events / campaigns e.g. Safer Internet Day
- reference to the relevant web sites/publications,
  e.g. SWGfL; *www.saferinternet.org.uk/*; *www.childnet.com/parents-and-carers* (see Appendix for further links/resources).
- Sharing good practice with other schools

Technology

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

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 and governors 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.

The filtering and monitoring provision is reviewed (at least annually) by senior leaders, the Designated Safeguarding Lead and a governor.

- checks on the filtering and monitoring system are carried out by the school 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."

- a member of the Leadership Team and a 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 schools internet provision. The filtering provided meets the standards defined in the DfE

Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre *Appropriate filtering.*

- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective. 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.
- There are regular checks of the effectiveness of the filtering systems . Checks are undertaken across a range of devices at least termly and the results recorded and analysed to inform and improve provision. The DSL and Governor are involved in the process and aware of the findings. (Schools may wish to use e.g. using SWGfL Testfiltering.com to carry out these checks)
- Devices that are provided by the school have school-based filtering applied irrespective of their location.
- 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.)
- 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 school follows the UK Safer Internet Centre Appropriate Monitoring guidance.

 The school has monitoring systems in place, agreed by senior leaders and technical staff, to protect the school, systems and users: Classroom Cloud is used by staff for monitoring purposes.

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.

Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended in the DfE Technical Standards for Schools and Colleges.

- 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 – all passwords must be at least 12 characters long
- 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 IT technician 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 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[1]	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	Yes	Yes	Yes
Full network access	Yes	Yes	Yes	Yes (separate V-Lan)	Yes	
Internet only						
No network access						Yes

School owned/provided devices:

- all school devices are managed though the use of Mobile Device Management software
- there is an asset log that clearly states whom a device has been allocated to. There is clear guidance on where, when and how use is allowed
- The Acorns Department is a mobile and any device that can take images or record (including wearables) free zone .
- personal use (e.g. online banking, shopping, images etc.) is clearly defined and expectations are well-communicated.
- the use of devices on trips/events away from school is clearly defined and expectation are well-communicated.
- liability for damage aligns with current school policy for the replacement of equipment.
- education is in place to support responsible use.

Personal devices:

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

Social Media

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

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

School staff should ensure that:

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

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

- a process for approval by senior leaders
- clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff
- a code of behaviour for users of the accounts
- systems for reporting and dealing with abuse and misuse
- understanding of how incidents may be dealt with under school disciplinary procedures.

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.
- 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. Any 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 children in the digital/video images
- staff and volunteers are allowed to take digital/video images on school devices 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
- 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
- Social media
- Online newsletters
- *Other (to be described)*

The school website is managed by Shrewsbury School Marketing Team 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 and ensures that where AI services are used, data privacy is prioritised.

Cyber Security

"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 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 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

Appendices

Copies of the more detailed template policies and agreements, contained in the appendix, can be found in the links and resources section of the relevant aspects in the 360safe self-review tool and online on the SWGfL website.

The appendices are as follows:

- A1 - Learner Acceptable Use Agreement Template – KS3
- A2 - Learner Acceptable Use Agreement Template – KS2
- A3 - Learner Acceptable Use Agreement Template – for younger learners (KS1)
- A4 - Parent/Carer Acceptable Use Agreement Template
- A5 - Staff (and Volunteer) Acceptable Use Policy Agreement Template
- A6 – Online Safety Group Terms of Reference Template
- A7 - Responding to incidents of misuse – flow chart
- A8 - Record of reviewing devices/internet sites (responding to incidents of misuse)
- A9 – Bring Your Own Device (BYOD) Policy
- A10 - Reporting Log
- B1 - Training Needs Audit Log
- Links to other organisations and resources
- Glossary of Terms

Appendix 1: Key Stage 3 Acceptable Use Policy and Form

I agree to use the school's digital systems responsibly to protect my safety, the security of the school systems, and others.

Personal Safety

- The school will monitor my use of its digital systems, devices, and communications.
- I will keep my usernames and passwords secure and private. If compromised, I will report or change them immediately.
- I will only share personal information, like my name or address, when absolutely necessary and with permission.
- I will be cautious when meeting online contacts in person, only doing so with a trusted adult in a public place.
- I will take responsibility for my actions online, using tools like blocking or ending chats if needed.
- I will share images of myself or others only when it is safe and will ensure the images are appropriate and respectful.
- I will only take or share images of myself, or others, when fully dressed. I understand that sharing nude or semi-nude content can cause distress, may be illegal and could lead to prosecution / criminal records.
- I will report harmful or unpleasant material, messages, or anything that worries or upsets me to a trusted adult.

Respecting Others' Work and Information

- I will seek permission before using or adapting someone else's work.
- I will verify information I find online, as it may not always be accurate or truthful.
- I will only use Artificial Intelligence (AI) tools approved by the school and ensure my use is ethical, legal, and transparent.
- I will fact-check and critically evaluate AI-generated content for accuracy, bias, and discrimination before sharing or publishing.
- I will avoid downloading or using copyrighted or protected materials without proper permission.

Responsible Online Behaviour

- I will be polite and responsible when I communicate with others. I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions. I will not bully, harass, threaten, upset or make fun of others.
- I will only use platforms or software approved by the school and will not attempt to bypass the filtering/security systems in place. If I become aware of any such attempts, I will report this to a trusted adult.
- I understand cybersecurity poses a risk to both me, other learners and the school and will ensure I take precautions before accessing emails, messages or links. I will check with trusted adults if I have any such concerns.
- I will immediately report any damage, faults or failings involving equipment or software, however this may have happened.
- I will follow the age requirements for social media, apps, and tools.
- I will balance my online and offline activities to promote a healthy lifestyle.
- I will protect my online reputation and that of the school, its staff, and other learners.
- I understand that some online behaviours might be regarded, by some, as fun but can have serious consequences – this might include taking (or sharing) images/videos of staff, fights, learners in embarrassing situations or the setting up of fake accounts.
- I will ensure my behaviour reflects positively on the school, both in and out of school settings.

Use of personal devices

- I understand that personal devices are only to be used in lessons, or when given special permission by a suitable adult.
- My device should be kept safe, either in a classroom or the charging cabinet.

- My device should be either locked in the charging cabinet, or signed out every evening.
- It is my responsibility to ensure my device is fully always charged and ready for use.

Consequences of Misuse

- I understand that failing to follow this agreement may lead to consequences, including loss of access to the school's systems, detentions, suspensions, contacting parents/carers, or involvement of the police in serious cases.

By following these guidelines, I will contribute to a safe, respectful, and productive online environment.

I have read and understand the above and agree to follow these guidelines when:

- I use the school's systems and devices (both in and out of school)
- I use my own devices in the school (when allowed)
- I use digital technologies out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, website etc.

Name: …………………………………….. Form:……………………

Date: ……………………………..

Appendix 2: Key Stage 2 Acceptable Use Policy and Form

I agree to use the school's digital systems safely and responsibly to protect me, other learners and the school.

Keeping Safe Online

- The school will check how I use devices and the internet to keep everyone safe.
- I will keep my usernames and passwords private and tell a trusted adult if someone else knows them.
- I will be careful when talking to people online and will only talk to people I know and trust.
- I will not share personal information like my name, address, or photos without asking a trusted adult.
- I will only take or share images of myself, or others, when fully dressed.
- If I see or hear something online that worries or upsets me, I will tell a trusted adult straight away.
- I will only meet people I have spoken to online if a trusted adult is with me.

Using Computers and the Internet Sensibly

- I will only use devices, apps and sites that I am allowed to, and will check if I am unsure.
- I will always ask permission and check with a trusted adult before using someone else's work or pictures.
- I will make sure the information I find online is true by checking carefully.
- I will only use apps or tools, like AI, that my teacher has said are OK, and I will ask for help if I'm unsure.
- I will not copy or use music, videos, or games unless I have permission.
- I will tell a trusted adult about any damage to devices or if anything else goes wrong.
- I will check with trusted adults before clicking on any unexpected messages or links (even if these look as though they are from people that I already know).

Being Respectful and Responsible

- I will treat others kindly online, just as I do in real life.
- I will make good choices about what I share online to protect myself and others.
- I will spend a healthy amount of time using devices and make time for other activities too.
- I will always think about how my behaviour online could affect me, my friends, and my school.

What Happens If I Break These Rules

- If I don't follow these rules, my teacher may stop me from using computers or devices, speak to my parents, or take other actions to help me make better choices in the future.

By following these rules, I can enjoy using technology safely and responsibly.
I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices.
- I use my own devices in the school (when allowed) e.g. mobile phones, etc ...
- I am out of school and involved in any online behaviour that might affect the school or other members of the school.

- Name: ……………………………………………… Form: …………………..

- Date: ……………………………………..

Appendix 3: Key Stage 1 Acceptable Use Agreement Form

Our Technology Rules

I will follow these rules to use computers, iPads and the internet safely at school.

Staying Safe

- My teacher will watch what I do on computers, tablets and the internet to keep me safe.
- I will keep my passwords secret and tell my teacher if I need help.
- I understand that people online are not always who they say they are. I will only talk to people online if my teacher or a trusted adult says it's OK.
- I will not share my name, address, or pictures without asking my teacher or a trusted adult first.
- If I see something that makes me feel worried or upset, I will tell my teacher or a trusted adult straight away.
- I will only use apps, games or websites my teacher says are safe.

Using Technology Kindly

- I will be kind when using technology, just like I am in real life.
- I will take care of the computers and iPads I use.
- I will only look at things my teacher says are OK.

Making Good Choices

- I will ask my teacher before I use someone else's pictures or work.
- I will take breaks from screens and do other fun things too.
- I know that I can say no / please stop to anyone online who makes me feel sad, uncomfortable, embarrassed or upset.
- I will ask for help from a trusted adult if I am not sure what to do or if I think I may have done something wrong.

What Happens If I Forget the Rules

- If I forget the rules, my teacher will help me learn to make better choices next time.

These rules help us all stay safe and have fun using computers and tablets at school!

Signed (child):

Signed (parent):

Appendix 4: Parent / Guardian Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open new opportunities for everyone. They can stimulate discussion, promote creativity, and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This acceptable use policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that learners have good access to digital technologies to enhance their learning and will, in return, expect the learners to agree to be responsible users. A copy of the learner acceptable use agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

KS2 and above

Your son/daughter has signed an acceptable use agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

KS1

The school has discussed the acceptable use agreement with your son/daughter and they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

The school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. The school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

Your son's/daughter's activity on the systems will be monitored and the school will contact you if they have concerns about any possible breaches of the acceptable use agreement.

Parents should encourage their child to adopt safe use of the internet and digital technologies at home and should inform the school if they have concerns over their child's online safety.

Use of Digital/Video Images

The use of digital/video images plays an important part in learning activities. Learners and members of staff may use school digital devices to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. Where an image is publicly shared by any means, only your child's first name/initials will be used unless you have told us that you do not wish your child's image to shared publicly.

The school will comply with the Data Protection Act and request parent's/carer's permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

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.

Parents/carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents/carers to agree.
As the schools is collecting personal data by issuing this form, it should inform parents/carers as to:

This form (electronic or printed)	The images
Who will have access to this form.	Where the images may be published. Such as; Twitter, Facebook, the schools website, local press, etc. (see relevant section of form below)
Where this form will be stored.	Who will have access to the images.
How long this form will be stored for.	Where the images will be stored.
How this form will be destroyed.	How long the images will be stored for.
	How the images will be destroyed.
	How a request for deletion of the images can be made.

Digital / Video Images Permission Form

As the parent/carer of the above learner, I agree to the school taking digital/video images of my child/children.	Yes/No
I agree to these images being used:	
• to support learning activities.	Yes/No
• in publicity that reasonably celebrates success and promotes the work of the school.	Yes/No
Insert statements here that explicitly detail where images are published by the schools	Yes/No
I agree that if I take digital or video images at, or of school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.	Yes/No

Use of Cloud Systems Permission Form

The school uses Microsoft 365 for learners and staff.

The following services, described below, are available to each learner as part of the school's online presence in Microsoft 365.

Using Microsoft 365 will enable your child to collaboratively create, edit and share files and websites for school related projects and communicate via email with other learners and members of staff. These services are entirely online and available 24/7 from any internet-connected computer.

The school believes that use of the tools significantly adds to your child's educational experience.

Pupil Acceptable Use Agreement

We have attached, for the information of parents and carers, the learner acceptable use agreement.

Appendix 5: Staff and Volunteer Acceptable Use Policy Agreement

School Policy
Digital technologies have become integral to the lives of everyone, including children and young people, both within schools and in their lives outside school. The internet and digital technologies are powerful tools, which can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. The school has the right to protect itself and its systems and all users should have an entitlement to safe access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure:

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

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

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to minimise the risk to the safety, privacy or security of the school community and its systems. I acknowledge the potential of digital technologies for enhancing learning and will endeavour to integrate them in a way that aligns with the school's policy, ethos and values.

For my professional and personal safety

- I understand that the school will monitor my use of school devices and digital technology systems
- I understand that the rules set out in this agreement also apply to use of these devices and technologies out of school, and to the transfer of personal/sensitive data (digital or paper based) out of the school
- I understand that the school devices and digital technology systems are primarily intended for educational use and that I will only use them for personal or recreational use within relevant school policies.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will store my passwords securely and in line with the school's relevant security policy.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

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

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

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

- I will abide by all relevant guidance and legislation (e.g., Keeping Children Safe in Education/UK GDPR)
- I will ensure that I am aware of cyber-security risks and that I will not respond to any communications that might put my/school data or systems at risk from attack
- When using AI systems in my professional role I will use these responsibly and:
- will only use AI technologies approved by the school
- will be aware of the risks of bias and discrimination, critically evaluating the outputs of AI systems for such risks
- to protect personal and sensitive data, I will ensure that I have explicit authorisation when uploading sensitive school-related information into AI systems
- will take care not to 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.
- ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance
- critically evaluate AI-generated outputs to ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing
- will use generative AI tools responsibly to create authentic and beneficial content, ensuring respect for individuals' identity and well-being
- When I use my personal mobile devices in school, I will follow the rules set out by the school, in the same way as if I was using school equipment. I will ensure that any such devices are protected by up-to-date anti-virus/anti-malware software and are free from viruses.
- When communicating in a professional capacity, I will only use technology and systems sanctioned by the school.
- I will not use personal accounts on school systems.
- I will exercise informed safe and secure practice when accessing links to content from outside of my organisation to reduce the risk of cyber security threats.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not access illegal, inappropriate or harmful content on school systems.
- I will not bypass any filtering or security systems that are used to prevent access to such content.
- I will not install or attempt to install unauthorised programmes of any type on a school device, nor will I try to alter device settings, unless this is allowed in school policies
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school Data Security Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that the data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software; however, this may have happened.

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

- I will ensure that I have appropriate permissions to use the original work of others in my own work and will reflect this with appropriate acknowledgements, particularly where AI has been used to generate content
- Where content is protected by copyright, I will not download or distribute copies (including music and videos).

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

- I understand that this acceptable use agreement applies to my use of digital technologies related to my professional responsibilities, within or outside of the school.
- I will ensure my use of technologies and platforms is in line with the school's agreed codes of conduct.

- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and in the event of illegal activities, the involvement of the Police.

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

Staff/Volunteer Name: …………………………………………
Signed……………………………………………………………
Date ……………………………………………………..

Appendix 6: Online Safety Group Terms of Reference

1. Purpose

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

2. Membership

1. The online safety group will seek to include representation from all stakeholders. The composition of the group should include:
   - SLT/DSL/OSL – Sue Rigby & Charlotte Jackson-Hutt
   - Teaching staff member – Steve Rigby (Head of Digital Learning) & one other
   - Support staff member – Jem Bayliss
   - Governor
   2. Parent – Adam Haythorn (also member of the support team)
3. Digital Leaders (2) – for advice and feedback. Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the committee to provide advice and assistance where necessary.
4. Committee members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.
5. Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature
6. When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities

3. Chairperson

The Committee should select a suitable Chairperson from within the group. Their responsibilities include:
- Scheduling meetings and notifying members
- Inviting other people to attend meetings when required
- Guiding the meeting according to the agenda and time available
- Ensuring all discussion items end with a decision, action or definite outcome
- Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary

4. Duration of Meetings

Meetings shall be held termly for a period no longer than one hour.

5. Functions

These are to assist the DSL/OSL (or other relevant person) with the following:
- To keep up to date with new developments in the area of online safety
- To (at least) annually review and develop the online safety policy in line with new technologies and incidents
- To monitor the delivery and impact of the online safety policy
- To monitor the log of reported online safety incidents (anonymous) to inform future areas of teaching/learning/training.
- To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of online safety. This could be carried out through:
  o Staff meetings
  o Pupil forums (for advice and feedback)
  o Governors meetings
  o Surveys/questionnaires for learners, parents/carers and staff
  o Parents evenings
  o Website/newsletters
  o Online safety events

- o Internet Safety Day (annually held on the second Tuesday in February)
    - o Other methods
- To ensure that monitoring is carried out of Internet sites used across the schools.
- To monitor filtering/change control logs (e.g. requests for blocking/unblocking sites).
- To monitor the safe use of data across the schools
- To monitor incidents involving cyberbullying for staff and learners

6. Amendments

The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all committee members, by agreement of the majority. The above Terms of Reference for Packwood School have been agreed.
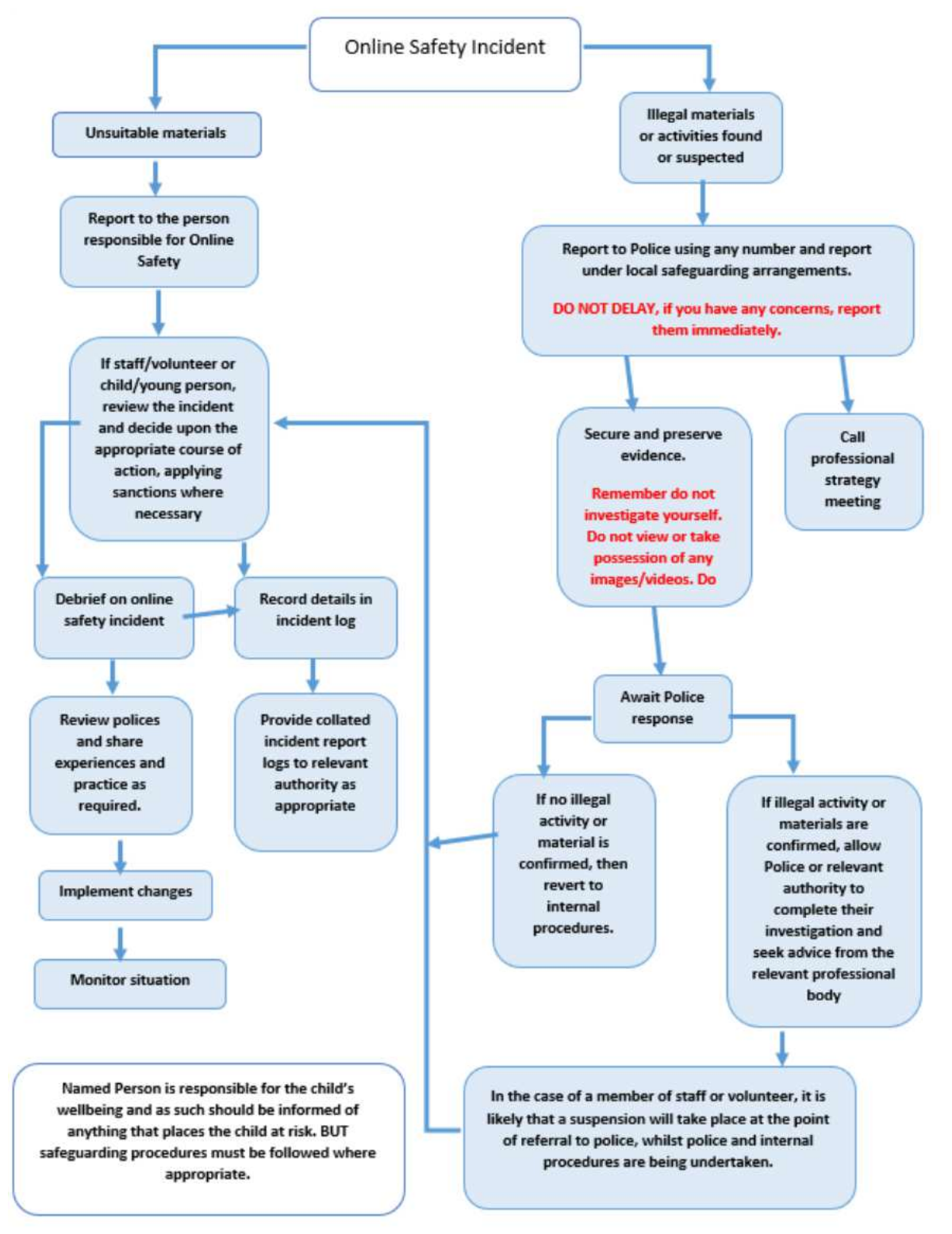
Signed by (SLT):   Date:

Date for review:

Acknowledgement. This template terms of reference document is based on one provided to schools by Somerset County Council

Appendix 7: Responding to Incidents of misuse – flow chart

Online Safety Incident

Unsuitable materials

Report to the person responsible for Online Safety

If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary

Debrief on online safety incident

Record details in incident log

Review polices and share experiences and practice as required.

Provide collated incident report logs to relevant authority as appropriate

Implement changes

Monitor situation

Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.

Illegal materials or activities found or suspected

Report to Police using any number and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.

Remember do not investigate yourself. Do not view or take possession of any images/videos. Do

Call professional strategy meeting

Await Police response

If no illegal activity or material is confirmed, then revert to internal procedures.

If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Appendix 8: Record of reviewing devices / internet sites (responding to incidents of misuse)

Group:
Date:
Reason for investigation:

Details of first reviewing person
Name:
Position:
Signature:

Details of second reviewing person
Name:
Position:
Signature:

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

Web site(s) address/device	Reason for concern

Conclusion and Action proposed or taken

Appendix 9: Bring Your Own Device Policy

For Years 7 and 8

What is our Digital Learning philosophy?

At Packwood we want to make sure that our pupils have the digital skills required to thrive here at Packwood and in their future education and on to the world of work. There is no doubt that being digitally literate is crucial for today's workforce. At Packwood we have a philosophy of a blended learning approach. This means that technology is integrated as part of normal lessons by teachers as they see fit and is just one of many approaches that we take to teaching and learning.

In order to facilitate this in the classroom for Years 7 and 8 Packwood operates a 1:1 policy meaning that each pupil needs to have their own device to access resources during the school day and beyond.

Device Security

- All devices should be clearly labelled.
- Pupils are responsible for ensuring that their device is in good working order at all times including charging.
- All devices are placed in the charging cabinets during free time.
- Any device that stays in school overnight is locked in the charging cabinet in the form room.
- It is advisable that an appropriate case is purchased for the device to provide protection.
- Parents are responsible for the insurance of the device.
- Whilst IT support are willing to help pupils who are having issues with their device, they are not responsible for fixing them and they cannot carry out any hardware repairs. This would need to be organised via your own means or through your insurance.

Equipment

The School recommends that the children purchase either a Surface Go 3 or the Surface Pro 9. Parents are recommended to take out their own insurance. The machines can purchased via Edutech and will delivered to school with a keyboard and a case. If a Surface is purchased independently the Surface must be purchased with Windows 11 Pro Edition to facilitate the integration into the School system.

All pupils should have their own headphones.

The Acceptable User Agreement Policy

The School takes cyber safety seriously. All pupils sign our Acceptable User Agreement annually and receive regular reminders of IT responsibilities, ethics and digital citizenship. We run enterprise-grade internet filtering to minimise inappropriate use and protect the school network. Pupils are therefore monitored when they connect to our wireless network.

Appendix 10: Reporting Log

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

Appendix 11: Training Needs Audit Log

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

Appendix 12: Links to organisations and helpful guidance

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

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

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

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

Bullying/Online-bullying/Sexting/Sexual Harassment
Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - http://enable.eun.org/
SELMA – Hacking Hate - https://selma.swgfl.co.uk
Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
Scottish Government - Better relationships, better learning, better behaviour - http://www.scotland.gov.uk/Publications/2013/03/7388
DfE - Cyberbullying guidance - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf
Childnet – Cyberbullying guidance and practical PSHE toolkit:
http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit
Childnet – Project deSHAME – Online Sexual Harrassment
UKSIC – Sexting Resources
Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm
Ditch the Label – Online Bullying Charity
Diana Award – Anti-Bullying Campaign

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

Curriculum
SWGfL Evolve - https://projectevolve.co.uk
UKCCIS – Education for a connected world framework
Department for Education: Teaching Online Safety in Schools
Teach Today – www.teachtoday.eu/
Insafe - Education Resources

Data Protection
360data - free questionnaire and data protection self review tool
ICO Guides for Organisations
IRMS - Records Management Toolkit for Schools
ICO Guidance on taking photos in schools

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

Infrastructure/Technical Support/Cyber-security
UKSIC – Appropriate Filtering and Monitoring
SWGfL Safety & Security Resources
Somerset - Questions for Technical Support
SWGfL - Cyber Security in Schools.
NCA – Guide to the Computer Misuse Act
NEN – Advice and Guidance Notes

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

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

Research
Ofcom –Media Literacy Research
Ofsted: Review of sexual abuse in schools and colleges

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

Appendix 13: Glossary of Terms

AUP/AUA	Acceptable Use Policy/Agreement – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of National Crime Agency, UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
FOSI	Family Online Safety Institute
ICO	Information Commissioners Office
ICT	Information and Communications Technology
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MAT	Multi Academy Trust
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational online safety programmes for schools, young people and parents.
UKSIC	UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.
UKCIS	UK Council for Internet Safety
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol

A more comprehensive glossary can be found at the end of the UKCIS [Education for a Connected World Framework](#)