Wincle CE Primary School

*Wincle School provides an enriching and outstanding rural education. We nurture the whole individual: body, mind and soul, inspiring rounded, happy, courageous children **who shine in all that they say and do**. Our children exhibit a passion for learning, a confident faith, a loving concern for community and an inclusive respect for all.*

Shine Like Stars' Philippians 2:15

Online Safety Policy	
Date updated:	**Brief summary of changes:**
October 2026	Policy reviewed with no inclusion of user agreements

Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of Wincle CE Primary School to safeguard members of our school community online in accordance with statutory guidance and best practice.
This Online Safety Policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).
Wincle CE Primary School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Legislative Framework

This policy has regard to:

- Keeping Children Safe in Education (current edition)
- Working Together to Safeguard Children (current edition)
- Education Act 2002
- Children Act 1989
- Children Act 2004
- Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR)
- Protection of Children Act 1978
- Counter-Terrorism and Security Act 2015
- The Prevent Duty Guidance
- The UK Safer Internet Centre Filtering and Monitoring Standards

Policy development, monitoring and review

This Online Safety Policy has been developed by the headteacher and staff and approved by the Governing Body.

Schedule for development, monitoring and review

This Online Safety Policy was approved by the school governing body on:	November 2026
The implementation of this Online Safety Policy will be monitored by:	Safeguarding Governor
Monitoring will take place at regular intervals: The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new	Annually

threats to online safety or incidents that have taken place. The next anticipated review date will be:	
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:	Annually
Should serious online safety incidents take place, the following external persons/agencies should be informed:	SCIES, Police.

Process for monitoring the impact of the Online Safety Policy
The school will monitor the impact of the policy using:
• logs of reported incidents
• monitoring logs of internet activity (including sites visited)
• internal monitoring data for network activity
• surveys/questionnaires of: learners, parents and carers, and staff.

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.

Headteacher

• The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding.
• The headteacher and the deputy DSL should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
• The headteacher is responsible for ensuring that the technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
• The headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out an internal online safety monitoring role.
• The headteacher will receive regular monitoring reports from the Online Safety Lead when the Lead is not the headteacher.

Governors

The DfE guidance “Keeping Children Safe in Education” states: “Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children’s welfare …. this includes … online safety”
Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy e.g. by asking the questions posed in the UKCIS document “Online Safety in Schools and Colleges – questions from the Governing Body”. This review will be carried out by the Pupil Welfare Subcommittee 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 Online Safety Lead
• regularly receiving (collated and anonymised) reports of online safety incidents
• checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
• reporting to relevant governors group/meeting

• membership of the school Safeguarding Group
• occasional review of the filtering change control logs and the monitoring of filtering logs (where possible)
The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

Online Safety Lead
The Online Safety Lead will:
• work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL), where these roles are not combined
• take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns
• have a leading role in establishing and reviewing the school online safety policies/documents
• promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
• liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
• ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
• receive reports of online safety incidents and create a log of incidents to inform future online safety developments
• provide (or identify sources of) training and advice for staff/governors/parents/carers/learners
• liaise with technical staff, pastoral staff and support staff
• meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and if possible, filtering and monitoring logs
• attend relevant governing body meetings/groups
• report regularly to headteacher.
• liaises with the local authority

Designated Safeguarding Lead (DSL)
The DfE guidance "Keeping Children Safe in Education" states: "The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety). This should be explicit in the role holder's job description." … Training should provide designated safeguarding leads with a good understanding of their own role, … so they … are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college."
The Designated Safeguarding Lead should be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:
• sharing of personal data
• access to illegal/inappropriate materials
• inappropriate online contact with adults/strangers
• potential or actual incidents of grooming

Curriculum Leads Curriculum
Leads will work with the Online Safety Lead to develop a planned and coordinated online safety education programme. This will be provided through:
• PHSE and SRE programmes
• A mapped cross-curricular programme
• assemblies and pastoral programmes
• through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

All staff working in schools need to know the 4 Cs (Keeping Children Safe in Education)

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and

Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/)

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 within the Staff Code of Conduct (AUA)
• they immediately report any suspected misuse or problem to the headteacher for investigation/action, in line with the school safeguarding procedures
• all digital communications with learners and parents/carers should be on a professional level and only carried out using official school systems
• online safety issues are embedded in all aspects of the curriculum and other activities
• ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
• they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
• in lessons where internet use is pre-planned learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
• where lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies.
• have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
• they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media

Network manager/technical staff – School IT Support

The network manager/technical staff is responsible for ensuring that

• they are aware of and follow the school Online Safety Policy to carry out their work effectively in line with school policy
• the school technical infrastructure is secure and is not open to misuse or malicious attack
• the school meets (as a minimum) the required online safety technical requirements as identified by the local authority
• there is clear, safe, and managed control of user access to networks and devices
• they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant

• the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the head for investigation and action
• the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
• monitoring software/systems are implemented and regularly updated as agreed in school policies.

Learners
• are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy (this should include 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
• should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents and carers
Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way. The school will take every opportunity to help parents and carers understand these issues through:
• publishing the school Online Safety Policy on the school website
• providing them with a copy of the learners' acceptable use agreement
• publish information about appropriate use of social media relating to posts concerning the school
• seeking their permissions concerning digital images, cloud services etc
• 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 use of their children's personal devices in the school (where this is allowed)

Pupil Safeguarding Group
This group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and monitoring the Online Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to senior leaders and the governing body.
Members of the Safeguarding Group will assist the Online Safety Lead with:
• the production/review/monitoring of the school Online Safety Policy/documents
• mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression and coverage
• 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

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

Acceptable use agreements
An Acceptable Use Agreement is a document that outlines a school's expectations on the responsible use of technology by its users. 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 code of conduct

• 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
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)					X

	• Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)					
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) Promotion of any kind of discrimination Using school systems to run a private business Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school Infringing copyright Unfair usage (downloading/uploading large files that hinders others in their use of the internet) 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 X X X X X	

Consideration should be given for the following activities when undertaken for non-educational purposes:	Staff and other adults				Learners			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permissi on
Online gaming	X				X			
Online shopping/commerce			X		X			
File sharing		X				X		
Social media Messaging/chat			X		X			
Entertainment streaming e.g. Netflix, Disney+			X	X	X			
Use of video broadcasting, e.g. YouTube, Twitch, TikTok			X	X				X
Mobile phones may be brought to school		X			X			
Use of mobile phones for learning at school	X				X			
Use of mobile phones in social time at school			X		X			
Taking photos on mobile phones/cameras				X	X			
Use of other personal devices, e.g. tablets, gaming devices	X				X			
Use of personal e-mail in school, or on school network/wi-fi		X						X

Use of school e-mail for personal e-mails	X				X			

When using communication technologies, the school considers the following as good practice:
• when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school
• any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content.
• 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 managing allegations policies.
• all members of the school community will be made aware of the need to report online safety issues/incidents
• reports will be dealt with as soon as is practically possible once they are received
• the Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
• if there is any suspicion that the incident involves any illegal activity or the potential for serious harm, the incident must be escalated through the agreed school safeguarding procedures.
• any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors
• where there is no suspected illegal activity, devices 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
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.

• 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
• learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously)

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



School actions

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

Online Safety Education Programme

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

• A planned online safety curriculum for all year groups matched against a nationally agreed framework and regularly taught in a variety of contexts.
• Lessons are matched to need; are age-related and build on prior learning
• Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
• 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 helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school
• staff should act as good role models in their use of digital technologies the internet and mobile devices
• in lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
• where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit
• it is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need
• the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

Artificial Intelligence (AI) and Deepfake Technology

The school recognises that Artificial Intelligence (AI) technologies, including generative AI tools, are becoming increasingly available to children and adults. Whilst these tools can support learning, creativity and productivity, they may also present safeguarding, data protection and educational risks. AI technologies may include, but are not limited to:

- AI-powered chatbots and assistants
- text generation tools
- image and video generation tools
- voice generation and voice-cloning software
- deepfake technology
- automated content creation systems

Pupils will be taught to use technology critically and responsibly, including understanding that AI-generated content may be inaccurate, biased, misleading or entirely fabricated.

The school will educate pupils about:

- identifying misinformation, disinformation and fake content;
- recognising deepfake images, videos and audio recordings;
- understanding that AI-generated content should not automatically be considered trustworthy;
- maintaining privacy and not sharing personal information within AI systems;
- the ethical and responsible use of AI technologies;
- the risks associated with AI-generated cyberbullying, impersonation, harassment and exploitation.

The creation, sharing or use of AI-generated content that causes harm to others, including deepfake images, manipulated videos, voice cloning, harassment, bullying, discriminatory content or sexually explicit material, will be treated as a serious breach of this policy and may be dealt with under the school's Behaviour Policy, Safeguarding and Child Protection Policy, Staff Code of Conduct and disciplinary procedures where appropriate.

Staff must not upload confidential, personal or sensitive school information into public AI systems unless authorised and compliant with the school's Data Protection Policy and data handling procedures.

Any safeguarding concerns involving AI-generated content, deepfakes, online impersonation or misuse of AI technology will be managed in accordance with the school's safeguarding procedures and reported to the Designated Safeguarding Lead (DSL).

Staff/volunteers

All staff will receive online safety training and understand their responsibilities. 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 and 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. The Online Safety Lead and Designated Safeguarding Lead (or other nominated person) will receive regular updates and by reviewing guidance documents released by relevant organisations

Governors

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

• attendance at training provided by the local authority or other relevant organisation (e.g., SWGfL)

• participation in school training / information sessions for staff or parents (this may include attendance at assemblies/lessons). A higher level of training will be made available to (at least) the Online Safety Governor.

Families

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

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

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

• the school filtering policies are agreed by senior leaders and technical staff and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours
• the school manages access to content across its systems for all users. The filtering provided meets the standards defined in the UK Safer Internet Centre Appropriate filtering.
• access to online content and services is managed for all users
• illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
• there are established and effective routes for users to report inappropriate content
• there is a clear process in place to deal with requests for filtering changes
• the school has (if possible) provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/learners, etc.)
• younger learners will use child friendly/age-appropriate search engines e.g. SWGfL Swiggle
• filtering logs are regularly reviewed and alert the school to breaches of the filtering policy, which are then acted upon.
• where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.
• access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice. If necessary, the school will seek advice from, and report issues to, the SWGfL Report Harmful Content site.

Monitoring

The school has monitoring systems in place to protect the school, systems and users:
• The school monitors all network use across all its devices and services.
• An appropriate monitoring strategy for all users has been agreed and users are aware that the network is monitored. There is a staff lead responsible for managing the monitoring strategy and processes.
• There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention. Management of serious safeguarding alerts is consistent with safeguarding policy and practice
• Technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon.

For more information on filtering and monitoring, please see Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)

Technical Security

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

- there will be regular reviews and audits of the safety and security of school technical systems
- servers, wireless systems and cabling are securely located and physical access restricted
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,
- all users have clearly defined access rights to school technical systems and devices.
- all users (adults and learners) have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security
- all school networks and system will be protected by secure passwords. Passwords must not be shared with anyone.
- the master account passwords for the school systems are kept in a secure place. It is recommended that these are secured using two factor authentications for such accounts
- passwords should be long.
- records of learner usernames and passwords for learners in Key Stage 1 or younger can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user. Password complexity for younger learners may be reduced (for example 6 character maximum) and should not include special characters. Where external systems have different password requirements the use of random words or sentences should be encouraged
- password requirements for learners at Key Stage 2 and above should increase as learners progress through school
- The headteacher is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.
- an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint (anti-virus) software. • an agreed policy is in place for the provision of temporary access of 'guests', (e.g., trainee teachers, supply teachers, visitors) onto the school systems
- an agreed policy is in place regarding the extent of personal use that users (staff / learners / community users) and their family members are allowed on school devices that may be used out of school
- an agreed policy is in place that allows staff to/forbids staff from downloading executable files and installing programmes on school devices
- an agreed policy is in place regarding the use of removable media (e.g., memory sticks/CDs/DVDs) by users on school devices.
- systems are in place that prevent the unauthorised sharing of personal data unless safely encrypted or otherwise secured.

Mobile technologies

The DfE guidance "Keeping Children Safe in Education" states: "The school or college should have a clear policy on the use of mobile and smart technology. Amongst other things this will reflect the fact many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school or college, sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content.

Schools and colleges should carefully consider how this is managed on their premises. Mobile technology devices may be school owned/provided or personally owned and might include smartphone, tablet, wearable devices, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school learning platform and other cloud-based services such as e-mail and data storage. All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme

Digital and video images

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

• when using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.

• staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes

• in accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other learners in the digital/video images

• staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images

• care should be taken when sharing digital/video images that learners are appropriately dressed

• learners must not take, use, share, publish or distribute images of others without their permission

• photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with Online Safety Policy

• learners' full names will not be used anywhere on a website or blog, particularly in association with photographs

• written permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media. Permission is not required for images taken solely for internal purposes

• parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy

• images will be securely stored in line with the school retention policy

• 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

The school website is managed/hosted by Wix. 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 learners work, images or videos are published, their identities are protected, and full names are not published. The school public online publishing provides information about online safety e.g., publishing the schools Online Safety Policy and acceptable use agreements; curating latest advice and guidance; news articles etc, creating an online safety page on the school website.

Outcomes

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

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

Learner Acceptable Use Agreement – for KS2

Introduction

Digital technologies have become integral to the lives of children and young people, both within and outside schools. These technologies are powerful tools, which open-up new opportunities for everyone. They can stimulate discussion, encourage creativity and stimulate awareness of context to promote effective learning. Learners should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended:

• to ensure that learners will have good access to devices and online content, be responsible users and stay safe while using digital technologies for educational, personal and recreational use
• to help learners understand good online behaviours that they can use in school, but also outside school
• to protect school devices and networks from accidental or deliberate misuse that could put the security of the systems and users at risk.

Acceptable Use Agreement

When I use devices, I must behave responsibly to help keep me and other users safe online and to look after the devices. For my own personal safety:

• I understand that what I do online will be supervised and monitored and that I may not be allowed to use devices in school unless I follow these rules and use them responsibly
• I will only visit internet sites that adults have told me are safe to visit
• I will keep my username and password safe and secure and not share it with anyone else
• I will be aware of "stranger danger" when I am online
• I will not share personal information about myself or others when online
• If I arrange to meet people off-line that I have communicated with online, I will do so in a public place and take a trusted adult with me
• I will immediately tell an adult if I see anything that makes me feel uncomfortable when I see it online.

I will look after the devices I use, so that the school and everyone there can be safe:

• I will handle all the devices carefully and only use them if I have permission.
• I will not try to alter the settings on any devices or try to install any software or programmes.
• I will tell an adult if a device is damaged or if anything else goes wrong.
• I will only use the devices to do things that I am allowed to do.

I will think about how my behaviour online might affect other people:

• When online, I will act as I expect others to act toward me.
• I will not copy anyone else's work or files without their permission.
• I will be polite and responsible when I communicate with others and I appreciate that others may have different opinions to me.
• I will not take or share images of anyone without their permission.

I know that there are other rules that I need to follow:
• Where work is protected by copyright, I will not try to download copies (including music and videos).
• When I am using the internet to find information, I should take care to check that the information is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
• I should have permission if I use the original work of others in my own work.

I understand that I am responsible for my actions, both in and out of school:
• I know that I am expected to follow these rules in school and that I should behave in the same way when out of school as well.
• I understand that if I do not follow these rules, I may be subject to disciplinary action.

Learner Acceptable Use Agreement Form
Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:
• I use the school systems and devices (both in and out of school)
• I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
• I am out of school and involved in any online behaviour that might affect the school or other members of the school.

Name of Learner: _____
Group/Class: _____
Signed: _____
Date: _____
Parent/Carer Countersignature_____

Learner Acceptable Use Agreement – for younger learners (Foundation/KS1)

This is how we stay safe when we use computers:
• I will ask a teacher or suitable adult if I want to use the computers/tablets
• I will only use activities that a teacher or suitable adult has told or allowed me to use
• I will take care of computers/tablets and other equipment
• I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
• I will tell a teacher or suitable adult if I see something that upsets me on the screen
• I know that if I break the rules I might not be allowed to use a computer/tablet

Signed (child): _____

Signed (parent): _____

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

Reporting Log

Date	Time	Incident	Action Taken		Incident reported by:	Signature
			What?	By whom?		