GREAT FINBOROUGH CHURCH PRIMARY

Online Safety & Acceptable Use Policy

Linked documents:
Safeguarding Policy & Child Protection Procedures
Information Management Policy
Data Protection Policy
Mobile Phone Policy

Prepared by:	C Nelson
Approved by:	Full Governing Body
Signature of Chair of Governors:	Liam Page
Status & Review Cycle:	Statutory Annual
Date Approved:	
Review Date:	September 2027

Acknowledgement: This policy has been developed using the SWGfL Online Safety template policies

Table of Contents

Contents

Introduction 5
Scope of the Online Safety Policy 5
Monitoring the impact of the policy 5
Policy & Leadership 6
Roles and Responsibilities 6
Headteacher and Senior Leaders: 6
Governors 6
Designated Safeguarding Lead 7
Online Safety Lead (OSL): 7
Curriculum Leads 7
Teaching and Support Staff 8
IT Service Provider / Technical staff: 8
Pupils: 8
Parents / Carers 9
Volunteers 9
Policy Statements – Education & Training 9
Online Safety Education Programme - Pupils 9
Staff / Volunteers 10
Governors 10
External Stakeholders 10
Working with parents / carers 11
Use of Artificial Intelligence (AI) 11
Policy statements 11
Safe use, data protection and security 12
Quality, fairness and integrity 12
Reporting, monitoring and accountability 12
Use in assessment and feedback 12
Misuse and disciplinary action 12
Technology 13
Technical Security – infrastructure / equipment 13
Filtering and Monitoring 13
Oversight and Review 14
Cyber Security 15
Data Protection 15
Technology Practice 16
Purpose 16
Device Management 16

Digital Content 16
Public Online Communications 17
Review 17
Outcomes 18
Acceptable use 18
Reinforcement 18
Acceptable/Unacceptable Actions 19
Unsuitable / inappropriate activities 19
Communication Technology best practice 23
Social Media - Protecting Professional Identity 23
Reporting and responding to incidents of misuse 23
Introduction 23
Reporting Concerns 24
Responding to Concerns 24
Recording and Monitoring 24
Illegal Incidents 24
Other Incidents 26
School Actions & Sanctions 26
Responding to Learner Actions 27
Responding to Staff Actions 28
Appendices 29
Appendix A: Pupil Acceptable Use Agreement – for older pupils (UKS2) 29
Appendix B: Pupil Acceptable Use Policy Class Agreement (LKS2) 31
Appendix C: Pupil Acceptable Use Policy Class Agreement – (KS1) 32
Appendix D1: Staff Acceptable Use Agreement 33
Appendix D2: Volunteer Acceptable Use Agreement 36
Appendix F: Record of reviewing devices / internet sites (responding to incidents of misuse) 39
Appendix G: Template Reporting Log 41
Appendix H: REPORT OF ONLINE SAFETY CONCERN 42
Appendix I: Staff Use of AI Acceptable Use Agreement 44
Appendix J: Effectiveness of Filtering and Monitoring - Annual Review Form 46
Appendix K: Technical Security Policy 47
Purpose 47
Scope 47
Policy Statement 47
Access Control and Authentication 47
System Security and Maintenance 47
Device Management 47
Supplier Management 47
Incident Management 48

Review and Training 48
Appendix L: Filtering and Monitoring Policy 49
Purpose 49
Scope 49
Roles and Responsibilities 49
Policy Statement 49
Filtering 49
Monitoring 50
Review and Training 50
Appendix M: Cyber Security Policy 51
Purpose 51
Scope 51
Policy Statement 51
Cyber Security Strategy 51
Supplier Management 51
Awareness and Education 51
Incident Response 51
External Assurance 51
Review 51
Appendix N: Public Online Communications Policy 52
Purpose 52
Scope 52
Policy Statement 52
Roles and Responsibilities 52
Creation of Public Online Accounts 52
Monitoring and Moderation 52
Professional Standards 53
Use of Images and Media 53
Personal Use and Association with the School 53
Handling Complaints and Abuse 53
Training and Awareness 53
Review and Continuous Improvement 53

Introduction

Keeping Children Safe in Education (KCSIE) requires Local Authorities, Multi-Academy Trusts and schools to ensure children are safeguarded from harmful and inappropriate online material, and that online safety is a running and interrelated theme across the whole-school safeguarding approach. This includes how online safety is reflected in relevant policies, the curriculum, staff training, the role of the DSL (and deputies), and parental engagement.

KCSIE describes online safety risks across four broad areas:

- Content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news) and conspiracy theories,
- Contact: being subjected to harmful online interaction with other users or generative AI applications that simulate this; 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: behaviour that increases likelihood of harm for example, making, sending and receiving explicit images, including those generated using AI, and online bullying, and
- Commerce: risks such as gambling, inappropriate advertising, phishing and financial scams

Schools in England are subject to increased scrutiny of online safety through inspection, and the Counter Terrorism and Security Act 2015 requires schools to protect learners from terrorist and extremist material online.

Where online safety concerns or incidents occur outside school and are known to the school, Great Finborough Church Primary School will respond in line with this policy and related procedures, including the school's Safeguarding, Behaviour and Anti-Bullying policies. Where appropriate, parents/carers will be informed of incidents involving inappropriate online behaviour that take place out of school.

Scope of the Online Safety Policy

This Online Safety Policy sets out how Great Finborough Church Primary School will safeguard members of our community online, in line with statutory guidance and best practice. The school is aware of the wider statutory requirements that informs this policy.

This policy applies to all members of the school community who access or use school digital systems, including staff, pupils, governors, volunteers, parents/carers, visitors and community users. It applies to use of school systems both on and off site, and refers out to other policies such as the Mobile Phone policy regarding the use of personal devices on the school site.

Monitoring the impact of the policy

The school will evaluate the effectiveness of this policy using evidence such as:

- Logs of reported online safety incidents
- Filtering and monitoring records
- Reviews of the effectiveness of the filtering systems
- Internal network activity monitoring data
- Surveys/questionnaires (as appropriate) of: Pupils, Parents/carers, Staff

Policy & Leadership

Roles and Responsibilities

Online safety is a shared responsibility. All members of the school community are expected to model safe, responsible behaviour, report concerns promptly and learn from incidents and good practice. The roles below clarify accountability.

Headteacher and Senior Leaders:

The Headteacher and Senior leaders set the culture and ensure that systems are effective. In line with KCSIE, the DSL holds day-to-day lead responsibility.

The Headteacher and Senior leaders will:

- Ensure the school meets its safeguarding duty of care to all members of the school community, including online safety, though the day to day responsibility for online safety will be delegated to the Online Safety Lead.
- Know and apply procedures for serious allegations involving staff (Headteacher plus at least one senior leader). (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR disciplinary procedures).
- Ensure that the Designated Safeguarding Lead (DSL) / Online Safety Lead (OSL), IT provider/technical staff and relevant colleagues are trained and able to fulfil their roles, and able to train other colleagues as relevant.
- Ensure that all staff receive appropriate online safety training which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.
- Ensure that children and taught about how to keep themselves and others safe online, recognising that effective education will be tailored to the specific needs and vulnerabilities of individual children.
- Put in place appropriate oversight and support for internal monitoring activity.
- Establish and receive periodic online safety reports, and act on emerging risks and themes.
- The DSL and Online Safety Lead to work together on the (at least annual) review of the effectiveness of filtering and monitoring systems and ensure that these are recorded. (form can be found in Appendix J)

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing/challenging its effectiveness. This will be carried out by the Curriculum Committee receiving regular information about online safety incidents and monitoring reports.

KCSIE requires governors to:

- Ensure that all staff undergo safeguarding and child protection training (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring – at induction and regularly updated.
- Ensure that children are taught about safeguarding, including in relation to online safety.
- Review the DfE Filtering and Monitoring Standards and discuss with IT staff and service providers what more needs to be done to support the school in meeting this standard.

The governing body will nominate an Online Safety Governor who will:

- Meet regularly with the DSL/OSL.
- Receive anonymised incident and monitoring summaries.
- Check delivery of key commitments (e.g., education, reporting, staff training).
- Have an understanding of filtering and monitoring and through regular review, assess the effectiveness of filtering and monitoring with SLT, DSL and IT provider, in line with KCSIE and DfE Filtering and Monitoring standards.
- Report to the relevant governor group/committee
- Undertake basic cyber security awareness training and support school cyber security oversight.

The Safeguarding Governor also has responsibility for the oversight of online safety, including supporting parent/carer and community engagement in online safety.

Designated Safeguarding Lead
KCSIE (Para 125) states that the DSL leads safeguarding and child protection, including online safety, and understands filtering and monitoring systems and processes. KCSIE requires this to explicit in the DSL's job description.

The DSL will:

- Lead safeguarding, including online safety, with clear responsibilities in their job description.
- Maintain up-to-date knowledge of online risks, filtering/monitoring and cyber security.
- Coordinate and record online safety concerns and incidents, escalating and referring in line with safeguarding procedures.
- Liaise with the SLT, the Online Safety Governor, the IT provider/technical staff and relevant external partners as required.
- Review anonymised incident patterns and filtering/monitoring information with the Online Safety Lead.
- With the OSL, lead the (at least annual) review of the effectiveness of filtering and monitoring systems and ensure that these are recorded. (form can be found in Appendix J)
- Report regularly to SLT and drive continuous improvement across relevant policies and practice, using evidence (e.g. incident data, monitoring, self-review etc).
- Ensure appropriate support for learners with SEND.

Online Safety Lead (OSL):

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents.
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- coordinates awareness, staff confidence and reporting readiness through appropriate training.
- works with teaching staff and curriculum leads to map, embed and evaluate online safety education.
- liaises with school technical staff.
- meets periodically with the Online Safety Governor to discuss current issues, and review incident logs.
- reports as required to Senior Leadership Team.
- monitors incident logs.
- consults stakeholders – including parents / carers and the pupils about the online safety provision
- maintains current knowledge of risks across content, contact, conduct and commerce.

Curriculum Leads

Curriculum leads will work with the DSL/OSL to deliver a planned online safety programme (e.g. ProjectEVOLVE) through appropriate channels, e.g. Computing, PSHE/RSE, other curriculum areas, assemblies/pastoral provision and national initiatives e.g. Safer Internet Day.

Teaching and Support Staff
All staff are expected to uphold professional standards online and contribute to a strong safeguarding culture. Staff will:

- Follow the Online Safety Policy, Safeguarding/Child Protection Policy and Technical Security Policy (Appendix K), and sign/comply with the Staff Acceptable Use Policy/ Agreement (AUP).
- Maintain professional boundaries (including online/remote learning).
- Ensure that all digital communications with pupils / parents / carers is on a professional level and only carried out using official school systems.
- Supervise learner use of technology and follow procedures for online safety issues.
- Monitor the use of the school's digital technologies, including mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- Ensure that pupils understand and follow the online safety and acceptable use policies.
- Embed online safety where appropriate; teach research skills, copyright and plagiarism awareness.
- Challenge harmful online behaviour and report concerns promptly.
- Report any suspected misuse or problem to the Headteacher and Online Safety Lead for investigation / action / sanction.
- Use only school-approved digital services and AI tools; protect data, apply UK GDPR, and verify AI outputs for accuracy/bias before use.
- Complete induction and annual training, with updates as needed; contribute to improvement by sharing learning and concerns.
- In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use wherever possible, and will report to IT technical staff any unsuitable material that is found in internet searches

IT Service Provider / Technical staff:
The IT provider supports leaders and the DSL to meet DfE filtering, monitoring and technical standards. Where services are outsourced, the school remains accountable.

The IT provider / Technical staff will:

- Maintain secure infrastructure and managed user access.
- Implement, maintain and update filtering and monitoring; provide reports; act on alerts and concerns.
- Support procurement, risk identification, reviews and checks with SLT/DSL.
- Ensure that the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- Monitor systems for misuse and report concerns promptly to the Headteacher.
- Follow the school's Online Safety and Technical Security (Appendix K) policies and keep technical knowledge current.

Pupils:
- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement.
- use technology responsibly, demonstrating a good understanding of research skills.
- understand the need to avoid plagiarism by upholding copyright regulations and respecting intellectual property.
- report concerns and know how to get help.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials, and know how to do so.
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- 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
- Use AI responsibly: protect original work, check accuracy and avoid plagiarism.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way and reinforcing safe online behaviour. The school will take every opportunity to help parents understand these issues. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and/or on-line pupil records
- ensuring that the school's policies regarding personal devices are followed.

Volunteers

Volunteers who access school systems as part of the wider school provision will be expected to sign the Staff and Volunteer AUA before being provided with access to school systems.

Policy Statements – Education & Training

Online Safety Education Programme - Pupils

Online safety education is a core part of the school's safeguarding approach and sits alongside effective technical controls (including filtering and monitoring). In line with KCSIE, online safety is a running and interrelated theme reflected across relevant policies and the curriculum.

The school delivers a broad, relevant, progressive and inclusive programme of online safety education for all learners, aligned to nationally recognised guidance and frameworks (including DfE "Teaching Online Safety in Schools", UKCIS "Education for a Connected World"). Learning is age-appropriate, builds on prior learning, is matched to need, and is taught through existing curriculum areas (including Computing and RSHE/RSE), with assessment and clear intended outcomes.

This approach will develop learners' ability to:

- adopt safe and responsible use of digital technologies, the Internet and mobile devices, both within and outside school, reinforced using good role modelling by staff;
- access appropriate sites and online material using recognised safe search engines;
- recognise and manage online risks, including harmful content, contact, conduct and commerce risks;
- understand consent, sexual harassment and sexual violence (including online), supported by safe opportunities for discussion;
- think critically about what they see online, including how to check and validate reliability and accuracy and the role of AI-generated content;
- respect copyright and intellectual property, including when using online material and AI tools;
- understand and follow the learner acceptable use agreement, and act within moral and legal boundaries (including awareness of the Computer Misuse Act 1990).

Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. In line with DfE Keeping Children Safe in Education (KCSIE), all staff and volunteers receive safeguarding and child protection training, including online safety, at induction and through regular updates (at least annually). Online safety training is integrated into the school's whole-school safeguarding approach, wider staff development and curriculum planning.

All staff will receive online safety training and understand their responsibilities under this policy. Training will include:

- A planned programme of online safety, data protection and cybersecurity training for all staff, regularly updated and reinforced. Staff training needs will be reviewed periodically to ensure provision remains relevant and effective.
- An understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring (KCSIE 2026).
- Online safety training for all new staff as part of induction, ensuring understanding of the Online Safety Policy and Acceptable Use Agreements, including classroom management, professional conduct, online reputation and modelling positive online behaviour.
- Regular updates for the Designated Safeguarding Lead and Online Safety Lead (or other nominated staff) through external training and review of relevant guidance (e.g. UK Safer Internet Centre, SWGfL, Local Authority or other appropriate organisations).
- Support for staff knowledge-building and consistent practice through structured professional learning resources (e.g. Project EVOLVE EDU) and, where appropriate, enhanced pathways (e.g. ProjectEVOLVE SAFEGUARDING).
- Regular review of this Online Safety Policy and updates through staff meetings, team briefings and/or INSET.
- Targeted advice, guidance and training from the DSL/OSL (or nominated staff) to individuals as required.

Governors

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

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organization;
- Participation in school training / information sessions for staff or parents;
- Regular update meetings with the DSL and/or Online Safety Lead to review key themes, incidents and current priorities.

External Stakeholders

Families, the wider community and external agencies play a vital role in supporting the online safety education and wellbeing of learners. The school recognises that parents and carers may have limited awareness of online risks, and that many external bodies can enhance the school's safeguarding approach. The school therefore works actively to build strong partnerships, share key messages, and ensure that families and the wider community are equipped to help keep children safe online.

Working with parents / carers

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 on-line 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 therefore support parents and carers to understand online risks, build confidence, and reinforce safe online behaviours at home, through:

- communication and awareness-raising about online safety issues and curriculum content.
- Providing information through newsletters, the school website, and digital communication tools.
- Involving learners in sharing online safety messages with parents/carers.
- Signposting parents and carers to trusted national resources (e.g. UK Safer Internet Centre, Internet Matters, Childnet).
- Promoting and participating in key national events such as Safer Internet Day.
- Ensuring parents and carers understand acceptable use expectations and relevant school policies related to online safety.

Use of Artificial Intelligence (AI)

Generative AI (Gen AI) is developing rapidly and its use in education is increasing. In schools, AI is typically used in three areas: learner support, teacher support, and school operations. All use must be safe, ethical and responsible.

We recognise that Gen AI can introduce risks. These risks can be reduced through our existing safeguarding, data protection and technical security arrangements, and by updating procedures where needed. Safeguarding of learners and staff remains central to our approach.

KCSIE 2026 recognises that learners may be subject to harmful online interaction with other users or generative AI applications that simulate these.

Policy statements

The school will:

- Support appropriate use of AI to enhance learning and teaching, improve outcomes, streamline administration and reduce workload. Staff remain professionally responsible and accountable for any work supported by AI.
- Comply with relevant law and guidance, including Keeping Children Safe in Education (KCSIE) and UK GDPR.
- Provide training and guidance for staff and governors on the benefits, risks and safe use of AI, and identify further development needs.
- Teach about AI through the curriculum where appropriate, helping learners understand how Gen AI works, its benefits and limitations, and its ethical and social impacts.

Safe use, data protection and security

The school will:

- Protect personal and sensitive data. Staff must not enter personally identifiable or sensitive information into AI tools. Where AI is used, staff should use anonymised data only.
- Require UK GDPR compliance. Staff must ensure any AI tool used meets data protection and security requirements before use.
- Approve tools and accounts. Only school-approved AI tools may be used for schoolwork, and staff should use school-provided AI accounts where available to support oversight and reduce risk.
- Safeguard sensitive information**.** Internal documents, strategic plans or other sensitive material must not be entered into third-party AI tools unless the tool and purpose have been explicitly approved.

Quality, fairness and integrity

The school will:

- Maintain human oversight. AI may support work but must not replace professional judgement—especially in decisions that affect people. AI outputs must be checked for accuracy before sharing or publishing.
- Promote transparency. Where AI has materially supported an output (e.g. documents, presentations, communications), staff should make this clear where appropriate.
- Address bias and discrimination. We recognise AI outputs may reflect bias. The school will use appropriate safeguards, review processes and procurement checks to prioritise fairness and safety.
- Protect copyright and intellectual property. The school will take steps to avoid copyright infringement and protect the intellectual property of staff and learners, including ensuring learners' work is not used to train AI systems without appropriate consent.

Reporting, monitoring and accountability

The school will:

- Require prompt reporting of AI-related concerns, including misuse, data incidents or inappropriate outputs, to the Headteacher
- Maintain an inventory of AI tools in use, with purposes and risks recorded, and carry out regular review.
- Engage parents/carers with clear information about how AI is used in school (e.g. an "AI in our school" guide).

Use in assessment and feedback

AI tools may be used to support teachers with assessment processes (e.g. identifying areas for improvement and drafting feedback), and to support learners in improving their work. Teachers remain responsible for outcomes and must ensure accuracy, fairness and appropriate use.

Misuse and disciplinary action

Improper use of AI—including breaches of this policy, data protection failures, misuse of sensitive information, or failure to follow agreed processes—may result in action under the school's Staff Disciplinary Policy.

*Appendix I provides an **AI-specific Staff Acceptable Use Agreement**.*

Technology

Purpose
The school recognises that effective filtering, monitoring, technical security, cyber security and data protection are essential to safeguarding children and protecting the wider school community. These measures support safe and responsible use of technology while enabling effective teaching, learning and administration.

Technical Security – infrastructure / equipment

The school will be responsible for ensuring that its technical infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. Internet access is via the school's broadband service provided by Suffolk County Council and the service is monitored by the Suffolk County Council Schools IT Services team. School staff will liaise with them as necessary.

The school ensures that:

- School technical systems will be managed in ways that ensure that the school meets its statutory technical requirements.
- There will be a review and audit of the safety and security of school technical systems when there are major system changes.
- Servers, wireless systems and cabling is securely located.
- Access to systems and data is controlled through appropriate authentication and permissions.
- The "master / administrator" passwords for the school ICT system are also available to the Headteacher and kept in a secure location.
- The Business Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Wireless encryption is used on all Access Points.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Temporary access for "guests" eg trainee teachers, supply teachers, and visitors into the school systems may be granted via the 'Teacher' user on school laptops.
- Staff issued with laptops that may be taken home should only use them for work related activities. Use of eBay, Facebook, developing personal websites, or activities related to a commercial business outside school are not allowed.
- Staff should only download executable files and install programs on school devices with the agreement of the Business Manager (or Headteacher in their absence).
- Personal data must not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
- Backups and recovery arrangements are in place to reduce the impact of system failure or attack.
- incidents and weaknesses are reported, recorded and used to inform improvement.

Filtering and Monitoring

The school has appropriate filtering and monitoring systems in place to help protect users from illegal, inappropriate and harmful online content and activity, in line with statutory guidance (e.g., DfE Technical Standards, DfE Generative AI: product safety standards; KCSIE) and best practice guidance (e.g., UKSIC Appropriate Filtering and Monitoring). The leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified.

The school ensures that:

- filtering and monitoring arrangements are safeguarding-led, proportionate and regularly reviewed
- filtering blocks illegal content and provides age-appropriate and role-appropriate access
- Internet access is filtered for all users. Illegal content is filtered by FortiNet, the filtering provider
- monitoring supports the rapid identification of safeguarding concerns and enables timely intervention
- School technical staff reserve the right to monitor and record the activity of users on the school technical systems, and users are made aware of this in the Acceptable Use Agreement.
- all school-owned devices are subject to filtering and monitoring, including when used off-site
- staff and learners understand that filtering and monitoring are in place, why they are needed, and how concerns are escalated
- where the use of personal devices is allowed, users understand that their use may be filtered and monitored by the school
- where Generative AI products are used they must effectively and reliably prevent users from accessing harmful or inappropriate content, and filtering mechanisms should be embedded within these products
- the technical limitations of the filtering system are understood, including whether the solution can monitor and filter real-time, dynamic, personalised or AI-generated content
- Any actual or potential technical incident / security breach should be reported to the Headteacher and the Business Manager.

Oversight and Review

- Senior leaders, the Designated Safeguarding Lead (DSL), technical staff and governors have clear roles and responsibilities
- Governors will review the DfE Filtering and Monitoring Standards and discuss with IT staff and service providers what needs to be done to support the school in meeting this standard.
- filtering and monitoring effectiveness is reviewed at least annually, and following significant changes or incidents. (e.g., using Testfiltering). Reviews will be carried out by the school's designated safeguarding lead, OSL, and technical support as appropriate. The review will include checks that filtering is working appropriately on all internet-connected devices in all relevant locations. Record of these checks will be kept and will include: when checks were conducted; which devices and environments were tested, issues identified and actions taken.
- log reports provide actionable information for safeguarding decisions.
- no system is relied upon in isolation; reporting routes and professional judgement remain central.

Further detail is provided in Appendix L - Filtering and Monitoring Policy

Cyber Security

The school recognises cyber security as a leadership and governance responsibility and takes steps to reduce the risk and impact of cyber incidents. (KCSIE 2026 refers to the DfE Cyber Security Standards and recognises cyber security as a safeguarding issue).

The school ensures that:

- a cyber security approach is in place to prevent, detect, respond to and recover from cyber threats
- senior leaders and governors understand cyber risks and their safeguarding implications receive appropriate assurance
- staff and learners are educated/trained to recognise and report cyber security concerns
- business continuity and incident response arrangements are maintained and reviewed
- cyber security arrangements are kept under regular review and updated in line with emerging risks.

Further detail is provided in the Appendix M – Cyber Security Policy.

Data Protection

The school is committed to protecting personal data and complying with data protection legislation. Personal data will be recorded, processed, transferred and made available according to GDPR and the Data Protection Act 2018.

(The Data (Use and Access) Act 2025 makes additional requirements on schools – particularly that online services accessed by pupils meet higher protection standards)

The school ensures that:

- personal data is processed lawfully, fairly and transparently
- a Data Protection Officer (DPO) is appointed and appropriate governance arrangements are in place
- personal data is accurate, adequate, relevant and not excessive, and is processed for limited purposes
- Personal data is kept no longer than is necessary, and is processed in accordance with the data subject's rights
- Personal data is only transferred to others with adequate protection
- all staff receive regular training to ensure they are aware of their responsibilities and can respond appropriately to data protection incidents.
- systems are in place to respond effectively to Freedom of Information and Subject Access Requests
- Data Protection Impact Assessments have been conducted on existing and planned use of software and systems.
- privacy notices explain how data is used and how individual rights can be exercised
- data is stored, shared and disposed of securely
- data breaches are reported and managed in line with legal requirements
- data protection is embedded across safeguarding, teaching, learning and administration
- where AI and Automated Decision-Making are in use, human oversight will be maintained for significant decisions, risk assessments will be conducted and the school will ensure automated systems are transparent and explainable.

See the *Data Protection* and *Information Management Policies*.

Technology Practice

Purpose

The school recognises that the safe and responsible day-to-day use of technology plays a vital role in safeguarding children, supporting learning, and protecting the school community. Clear expectations, consistent practice and informed users help reduce risk while enabling positive and purposeful use of digital technologies.

This approach supports the safeguarding duties set out in *Keeping Children Safe in Education*, emphasising safeguarding and whole-school responsibility, including the requirement to address online safety through policy, practice and education.

Detailed arrangements are set out in the Appendix K - Technical Security Policy and Appendix N – Public Online Communications Policy

Device Management

The school manages the use of digital devices in a way that supports safeguarding, learning and responsible behaviour. This reflects KCSIE's requirement for a clear mobile / smart technology policy and explicitly links device use to behaviour, safeguarding and education.

The school ensures that:

- expectations for the use of school-owned and personal devices are clearly defined and communicated
- device use is consistent with safeguarding, behaviour, data protection and acceptable use policies
- appropriate technical and procedural controls are in place to support safe use
- staff, learners and visitors have been trained/educated/informed and understand their responsibilities when using devices on school premises or systems
- education on the safe and responsible use of devices forms part of the school's online safety education
- As part of the mobile phone policy, and in line with the DfE statutory guidance, the school prohibits for learners the use of mobile phones and other smart technology with similar functionality to mobile phones throughout the school day, including during lessons, the time between lessons, breaktimes and lunchtime.

Decisions about device use are informed by risk assessment and reviewed regularly.

Detailed information and guidelines regarding the use of personal mobile technology in school can be found in the school's Mobile Phone Policy.

Digital Content

The school recognises that digital content (images, video and any other multi-modal digital media) can enrich learning and communication when used responsibly. It directly supports KCSIE expectations around sexual imagery, sharing of images, consent and coercion. It also reinforces lawful management of digital content as part of safeguarding and embeds education and prevention alongside policy.

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying 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 ensures that:

- clear expectations are in place for the creation, use, storage and sharing of digital content
- consent, privacy and safeguarding considerations are applied consistently
- staff and learners are trained/educated to understand their responsibilities when creating or sharing digital content
- personal data and images are handled securely and lawfully
- policy and practice are reviewed in the light of emerging technologies and risks.
- pupils are educated about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- appropriate care is taken when photographing/videoing pupils, ensuring that they are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- pupils must not take, use, share, publish or distribute images of others without their permission

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by GDPR and the Data Protection Act 2018). To respect everyone's privacy and in some cases protection, these images must not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils 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, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes. In the event that it is necessary to use a personal device, the business manager or online safety co-ordinator should be notified, a log of the details made, and the images transferred to a school system and removed from the personal device as soon as possible.

Public Online Communications

The school uses public online communications to inform, celebrate success and engage with the wider community, while managing associated risks. It supports KCSIE expectations around professional boundaries and staff conduct online, addresses reputational and safeguarding risk from public platforms while reinforcing parental engagement and transparency. It has considered the risks of AI manipulation of images as highlighted in the UK Online Harms Early Warning group guidance on Protecting your setting's images from AI manipulation and abuse.

The school ensures that:

- public online communications are appropriate, accurate and well-managed
- public communications from or regarding the school are monitored and addressed where appropriate
- published content complies with safeguarding, data protection and statutory requirements
- to reduce the risk of illegal manipulation of publicly available images of staff and learners, the school has procedures in place to control how those images are shared online. (guidance is available from UKSIC)
- online safety information is shared with parents, carers and the wider community
- clear processes exist for managing school online accounts
- staff understand expectations around professional conduct and online behaviour
- photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' 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 pupils are published on the school website

Review

Technology practice is reviewed regularly to reflect:

- changes in technology and online behaviour
- emerging safeguarding risks
- feedback from staff, learners and parents
- national guidance and statutory expectations

Outcomes

The impact of the Online Safety Policy and practice is evaluated regularly using evidence such as online safety incident logs, behaviour and bullying records, and surveys of staff, learners and parents/carers. Evaluating student outcomes as part of their online safety should be defined and evaluated as part of the school's assessment processes (e.g. using ProjectEVOLVE Knowledge Maps assessment and tracking). Findings are reported to relevant groups and used to strengthen practice.

This process ensures that:

- Evidence from audits and reviews is discussed through balanced professional debate, alongside the impact of preventative work (education, awareness and training).
- Clear reporting routes are in place so patterns, themes and outcomes are shared regularly with senior leaders and governors.
- Parents/carers are informed of key patterns and learning through the school's online safety communication and awareness activity.
- Online safety and related policies and procedures are updated in response to evidence and emerging risks.
- Learning and evidence of impact are shared, where appropriate, with other schools, agencies and local authorities to support a consistent local approach to online safety

Acceptable use

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies 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 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.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Acceptable use is defined through the Online Safety Policy and a suite of Acceptable Use Agreements (AUAs) *(see appendices).* AUAs matter most when they are understood, reinforced and followed—not simply signed.

Reinforcement

- staff and learner induction/handbooks
- posters in areas where technology is used
- curriculum and awareness sessions
- communications with parents/carers
- school website
- peer support / learner-led activity

Acceptable/Unacceptable Actions

The tables which follow detail acceptable/unacceptable actions when using digital technology.

Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

User actions		**Acceptable**	**Acceptable at certain times**	**Acceptable for nominated users**	**Unacceptable**	**Unacceptable & illegal**
Users must not use online services (apps, games, sites) to create, share, download, upload, transfer or communicate material or comments that are:	Any illegal activity, for example: • Child sexual abuse imagery (CSAM)* • Child sexual abuse/exploitation and grooming • Terrorism-related content • Encouraging, promoting or assisting suicide/self-harm • Sexual image offences (including intimate image abuse/revenge porn and extreme pornography) • Incitement to, or threats of, violence or mental harm • Hate crime • Public order offences (including harassment and stalking) • Drug-related offences • Weapons/firearms offences • Fraud and financial crime (including money laundering) • *Note: follow UKSIC and UKCIS guidance when responding to self-generated intimate images (SGII).*					X

User actions		**Acceptable**	**Acceptable at certain times**	**Acceptable for nominated users**	**Unacceptable**	**Unacceptable & illegal**
Users must not attempt or support cybercrime (Computer Misuse Act 1990), including:	• Misusing someone else's username/ID or password to access data, software or systems without authorisation • Gaining unauthorised access to school networks, data or files (including bypassing security controls) • Creating, introducing or spreading malware (viruses, ransomware, harmful scripts) • Phishing, credential theft, or attempting to capture passwords or personal data • Revealing, copying or publishing confidential information (e.g., personal/financial data, databases, access codes) • Disabling, impairing or disrupting network/services (e.g., denial of service) • Using penetration-testing tools without explicit permission *Note: schools should decide whether incidents are dealt with internally or reported to police. Serious or repeat offences should be reported. The National Crime Agency provides routes to divert young people away from cybercrime* and into positive pathways.					X
Unacceptable (not illegal) under school policies, for example:	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	
	Promoting discrimination, harassment or hateful content				X	
	Using school systems to run a private business or make unauthorised financial gain				X	
	Using tools/services to bypass filtering, monitoring or other safeguards (e.g., VPN/proxy, anonymisers, alternative DNS)				X	
	Infringing copyright or intellectual property (including via AI tools, stream ripping or unauthorised copying/sharing)				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Sharing content that is offensive, undermines the school's ethos, breaches integrity, or brings the school into disrepute				X	

The table below details the extent to which the following activities are allowable.

	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 oversight
Online gaming and in-game chat/voice (*e.g. Roblox, Fortnite, Minecraft*)	X				X			
Online shopping and digital commerce (*including in-app purchases, marketplaces, subscriptions)*				X	X			
Cloud storage and file sharing (*e.g., Google Drive, OneDrive, Dropbox, WeTransfer; P2P/torrents*)		X						X
Social media and user-generated platforms (**only to be used for school purposes**) *(e.g. TikTok, Instagram, Snapchat, X, Reddit) and other age-restricted services*			X		X			
Messaging, chat and voice (**only to be used for school purposes**) *(e.g., WhatsApp, iMessage, Snapchat, Discord, Teams personal accounts)*			X		X			
Streaming entertainment/media (video, music, podcasts) *e.g. Netflix, Disney+, Spotify*		X						X
Video platforms and livestreaming *(e.g. YouTube, Twitch, TikTok LIVE, Instagram Live)*		X						X
Personal mobile phones and smart devices on site *(phones, smartwatches, earbuds). N.b Smartphone bans in schools in England)* *Refer to the school's Mobile Phone Policy for more detailed information and guidance.*		X			X			

	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 oversight
Taking photos/video/audio on personal devices (including sharing, location data and consent)			X		X			
Other personal devices - for work purposes only *(e.g., tablets, handheld consoles, VR headsets, wearables)*		X					X	
Personal email accounts on site or on the school network/Wi-Fi *(e.g., Gmail, Outlook.com)*				X	X			
School email used for personal communication (non-work/non-learning)	X				X			
AI tools/services (generative AI chatbots and image/video tools, AI companions, browser extensions)			X					X

Communication Technology best practice

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

- Users should be aware that email communications may be monitored. Staff and pupils should therefore use only the school email service to communicate with others on school business.
- Users must immediately report, to the Headteacher or Business Manager 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.
- Any digital communication between staff and pupils or parents / carers must be professional in tone and content. These communications may only take place on official school systems. Personal email addresses or social media must not be used for these communications. In certain circumstances, e.g.,on school trips, text messaging is permitted, but the school text messaging system should be used in preference wherever possible.
- Whole class / group email addresses may be used within the school, where appropriate.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website, and only official email addresses should be used to identify members of staff or governors.

Social Media - Protecting Professional Identity

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

School staff should ensure that:

- No reference should be made in social media to pupils, 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 or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Reporting and responding to incidents of misuse

Introduction

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

The school is committed to creating a culture where all members of the community feel confident, safe, and supported in reporting online safety concerns. In line with *Keeping Children Safe in Education (KCSIE)*, the school recognises that online risks may occur in school or outside school and may affect children in any setting. Reporting routes must therefore be clear, accessible, inclusive, and consistently understood by all.

The school recognises national findings, including the Ofsted *Review of Sexual Abuse in Schools and Colleges* (2021), which highlight that children may not always feel able to report. The school assumes that harmful online behaviours may be occurring, even where none have been disclosed, and responds by maintaining strong systems for reporting, analysing, and addressing concerns. KCSIE suggests that staff should have a professional curiosity and speak to the designated safeguarding lead (or a deputy) if they have concerns about a child.

Reporting Concerns

The school will ensure that:

- Clear, accessible reporting routes are in place for all members of the school community, including pupils, staff, governors, parents/carers, and volunteers.
- Reporting processes are fully aligned with safeguarding procedures, including the child protection, whistleblowing, managing allegations and complaints policies.
- Multiple reporting options are available, such as speaking with the Designated Safeguarding Lead (DSL), online or anonymous reporting tools (e.g., Whisper), email contact, or in-person disclosures.
- Reporting routes are well publicised through induction, assemblies, posters, and the school website.
- All users understand that any online safety concern must be reported, including those relating to harmful or illegal behaviour, sexual harassment, bullying, discrimination, grooming, or self-generated sexual imagery.

Responding to Concerns

The school will ensure that:

- Reports are acknowledged and responded to promptly, considering the safety and wellbeing of the person reporting.
- The DSL, Online Safety Lead, and senior leaders have the training and skills needed to recognise, assess, and manage online safety risks.
- Where a report indicates possible illegal activity or serious harm, it is escalated immediately through safeguarding procedures. Examples include (but are not limited to):
    - Child sexual abuse material (CSAM)
    - Non-consensual or self-generated images
    - Grooming, exploitation, or sexual harassment
    - Terrorism or extremism
    - Hate crime, fraud, extortion, stalking
    - Cyber offences under the Computer Misuse Act
    - Sale of illegal substances or goods
- Where concerns do not involve suspected illegal activity, devices may be checked using a safe, controlled, and documented process involving senior staff and a designated review device.
- AI-supported monitoring systems, where used, are subject to human oversight to ensure contextual understanding.
- Users who report concerns receive reassurance, appropriate support, and feedback on the outcome.

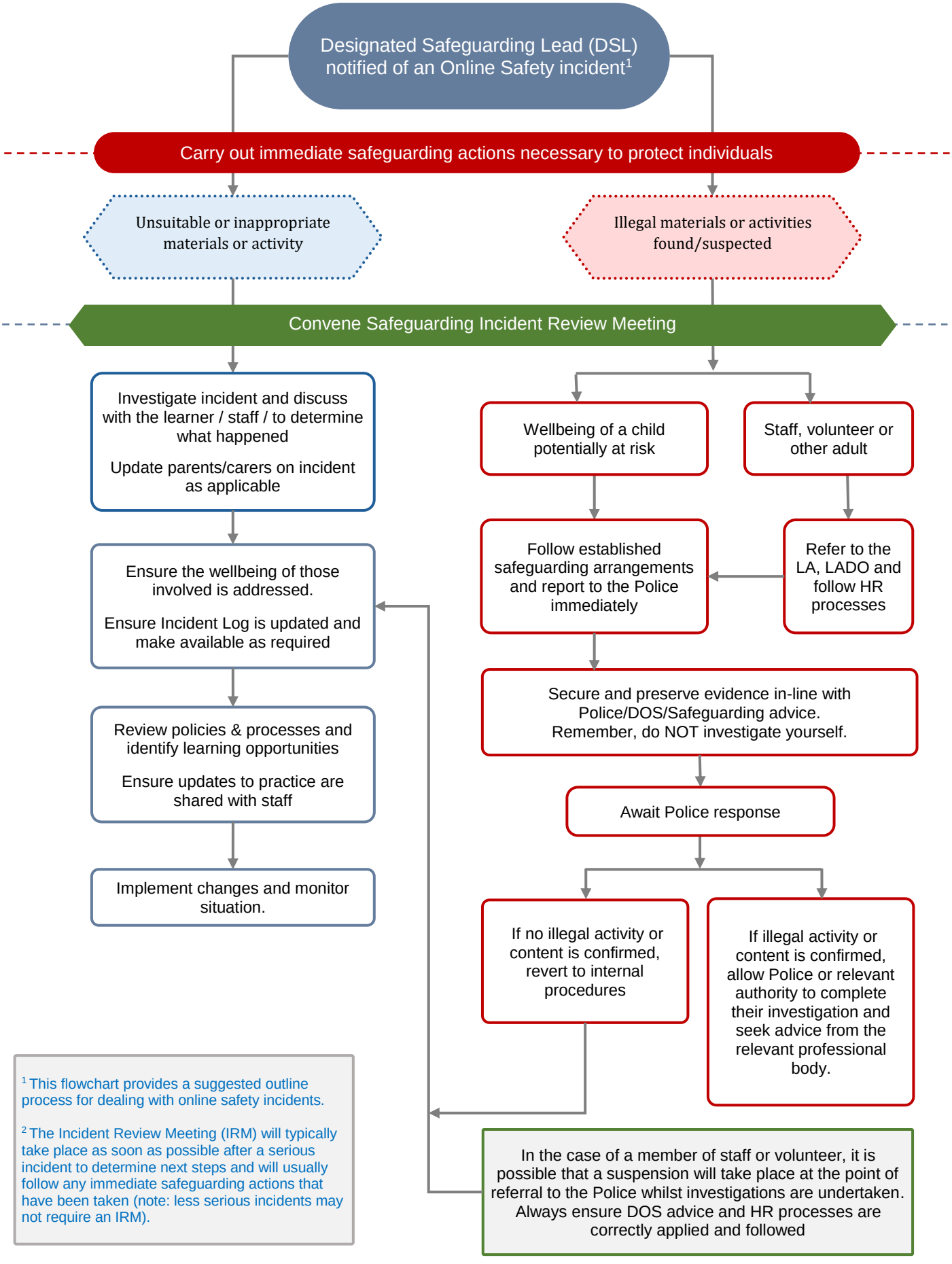
Recording and Monitoring

The school will:

- Maintain a secure and confidential record of all incidents, including actions, decisions, and follow-up.
- Ensure reports are audited and analysed regularly to identify emerging trends, patterns of concern, and the effectiveness of responses.
- Provide anonymised summaries of trends and learning to:
    - Senior leaders
    - Governors (via safeguarding reports)

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix E) for responding to online safety incidents and report immediately to the police.


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

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should 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 (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action

If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police, and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

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

Responding to Learner Actions

Incidents	Refer to class teacher	Refer to DSL / OSL	Refer to Headteacher	Refer to Technical Support Staff for action re: filtering /	Inform parents/carers	Issue a warning / intervention	Remove device / network /internet / access rights	Further sanction, in line with behaviour policy	Refer to Police/Social Services
Accessing illegal material (or attempting to), as defined in the earlier "Unsuitable/Inappropriate Activities" section.	X	X	X						X
Unauthorised access to the school network, including using another person's account or sharing usernames/passwords.	X	X	X	X					
Damaging, corrupting or deleting another user's data.	X	X	X	X					
Sending offensive, harassing or bullying emails, texts or messages.	X	X	X	X					
Unauthorised downloading / uploading, file sharing or distribution of files.	X	X	X	X					
Bypassing filtering (e.g. proxy sites, VPNs or similar tools).	X	X	X	X					
Failing to report accidental access to offensive or pornographic material	X	X	X	X	X	X			
Deliberately accessing offensive or pornographic material (or attempting to)	X	X	X	X	X			X	
Sharing or receiving content that breaches copyright or data protection law.	X	X	X		X	X	X	X	
Unauthorised use of devices, including taking photos/videos or audio recordings and using a smartphone in school *Also refer to the school's Mobile Phone Policy for more detailed information and guidance.*	X	X	X						
Unauthorised use of online services (apps, websites or platforms, including social media, messaging apps and personal email). N.b. this may need to be updated in response to the expected social media ban for U16s.	X	X	X	X					
Any online behaviour that could bring the school into disrepute or undermines the school's ethos.	X	X	X				X		
Repeated breaches of these rules following previous warnings or sanctions.					X	X	X	X	

Responding to Staff Actions

Incidents	Refer to SLT/Headteacher	Refer to Technical Support Staff for action re: filtering / security etc	Refer to HR	Issue a warning	Further Disciplinary action in line with Behaviour Policy	Refer to Local Authority	Refer to Police / LADO
Accessing illegal material (or attempting to), as defined in the earlier "Unsuitable/Inappropriate Activities" section.	X		X			X	X
Breaching data protection or cyber-security requirements, including network security rules.	X		X	X			
Accessing offensive or pornographic material (or attempting to).	X	X	X		X	X	
Damaging systems or data, including corrupting/deleting others' data or deliberately damaging hardware/software.	X		X	X			
Bypassing filtering controls (e.g. proxy sites, VPNs or similar methods).	X	X	X	X	X	X	
Unauthorised downloading, uploading or file sharing.	X	X	X	X			
Breaching copyright, licensing or intellectual property, including misuse of AI systems.	X		X	X			
Unauthorised account/network access, including sharing passwords, using another person's account, or allowing others access.	X	X	X	X			
Sending offensive, harassing or bullying emails, texts or messages.	X		X		X	X	
Use of personal email/social media/messaging to communicate with learners or parents/carers.	X		X		X	X	
Inappropriate personal use of school technology, including personal email and social media use during work time/using school systems.	X		X				
Mishandling personal data, including storing, displaying or transferring it insecurely.	X		X	X			
Any action that undermines professional conduct or a staff member's professional standing.	X		X	X			
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.	X		X	X			
Failing to report incidents, whether accidental or deliberate.	X		X	X			
Repeated breaches following previous warnings or sanctions.	X					X	

Appendices

The appendices below can be found on the following pages:

- Appendix A: Pupil Acceptable Use Agreement (UKS2)
- Appendix B: Pupil Acceptable Use Agreement (LKS2)
- Appendix C: Pupil Acceptable Use Agreement (EY/KS1)
- Appendix D1: Staff Acceptable Use Agreement Policy
- Appendix D2: Volunteers Acceptable Use Agreement Policy
- Appendix E: Responding to incidents of misuse – flowchart
- Appendix F: Record of reviewing sites (for internet misuse)
- Appendix G: School Reporting Log
- Appendix H: Online Safety Concern Reporting Form (Blue)
- Appendix I: Staff Use of AI Acceptable Use Agreement
- Appendix J: Effectiveness of Filtering and Monitoring - Annual Review Form
- Appendix K: Technical Security Policy
- Appendix L: Filtering and Monitoring Policy
- Appendix M: Cyber Security Policy
- Appendix N: Public Online Communications Policy

Appendix A: Pupil Acceptable Use Agreement – for older pupils (UKS2)

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 not use my own personal devices in school (including mobile phones, tablets, laptops and smart watches).
- 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 (both in and out of school)
- 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: ..... Class: .....

Signed: ..... Date: .....

Appendix B: Pupil Acceptable Use Policy Class Agreement (LKS2)

This acceptable Use Agreement is to be agreed and signed by all children in Years 3 and 4.

Our Technology Rules

I will follow these rules to use computers, tablets and the internet safely at school. These rules help us all stay safe and have fun using computers and tablets 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 tablets 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.

Signed (children):

Appendix C: Pupil Acceptable Use Policy Class Agreement – (KS1)

This acceptable Use Agreement is to be agreed and signed by all children in Years 1 and 2.

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
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of the computer 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.

Signed (children):

Appendix D1: Staff Acceptable Use 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. Great Finborough Church Primary 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.

The school expects that all colleagues will behave responsibly, with courtesy and sensitivity to others at all times, including when using technology. Colleagues are required to act in line with the Code of Conduct and this agreement.

This acceptable use policy is intended to ensure:

- that staff 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.

Great Finborough Primary School will try to ensure that staff will have good access to digital technology to enhance their work, to enhance learning opportunities and will, in return, expect staff 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. I will, where possible, educate the learners in my care in the safe use of digital technologies, and embed Online Safety in my work.

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 school in accordance with school policies. I will not invite pupils onto social networking sites, or accept invitations from them. If I communicate with parents or other members of the school community on social media, I will maintain professional boundaries.
- I will only communicate with learners and parents/carers, or conduct school business with third parties, 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 in this agreement and 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 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 try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install unauthorised programs of any type on a school device, nor will I try to alter device settings, unless this has been agreed by the headteacher.
- 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 Protection (including Data Security) and Information Management Policies. 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 digital technologies 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/or the Local Authority, 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 Name: .....

Signed: .....

Date: .....

Appendix D2: Volunteer Acceptable Use 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. Great Finborough Church Primary 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.

The school expects that all colleagues will behave responsibly, with courtesy and sensitivity to others at all times, including when using technology. Colleagues are required to act in line with the Volunteer Code of Conduct and this agreement.

This acceptable use policy is intended to ensure:

- that 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 volunteers are protected from potential risk in their use of technology in their everyday work.

Great Finborough Primary School will try to ensure that volunteers will have good access to digital technology when needed to support their work in school and, in return, expect 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, when working with learners, model good practice in Online Safety.

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.
- I will only use social networking sites in school in accordance with school policies.
- I will not engage in any online activity that may compromise my role as a volunteer.

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.
- I will not use any personal devices when working in school unless this has been previously agreed by the Headteacher.
- 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 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 programs of any type on a school device, nor will I try to alter device settings.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will not transport, hold, disclose or share personal information about myself or other members of the school community, as outlined in the school Data Protection (including Data Security) and Information Management Policies.
- 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 digital technologies in my volunteer 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 volunteer 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/or the Local Authority, and in the event of illegal activities, the involvement of the Police.

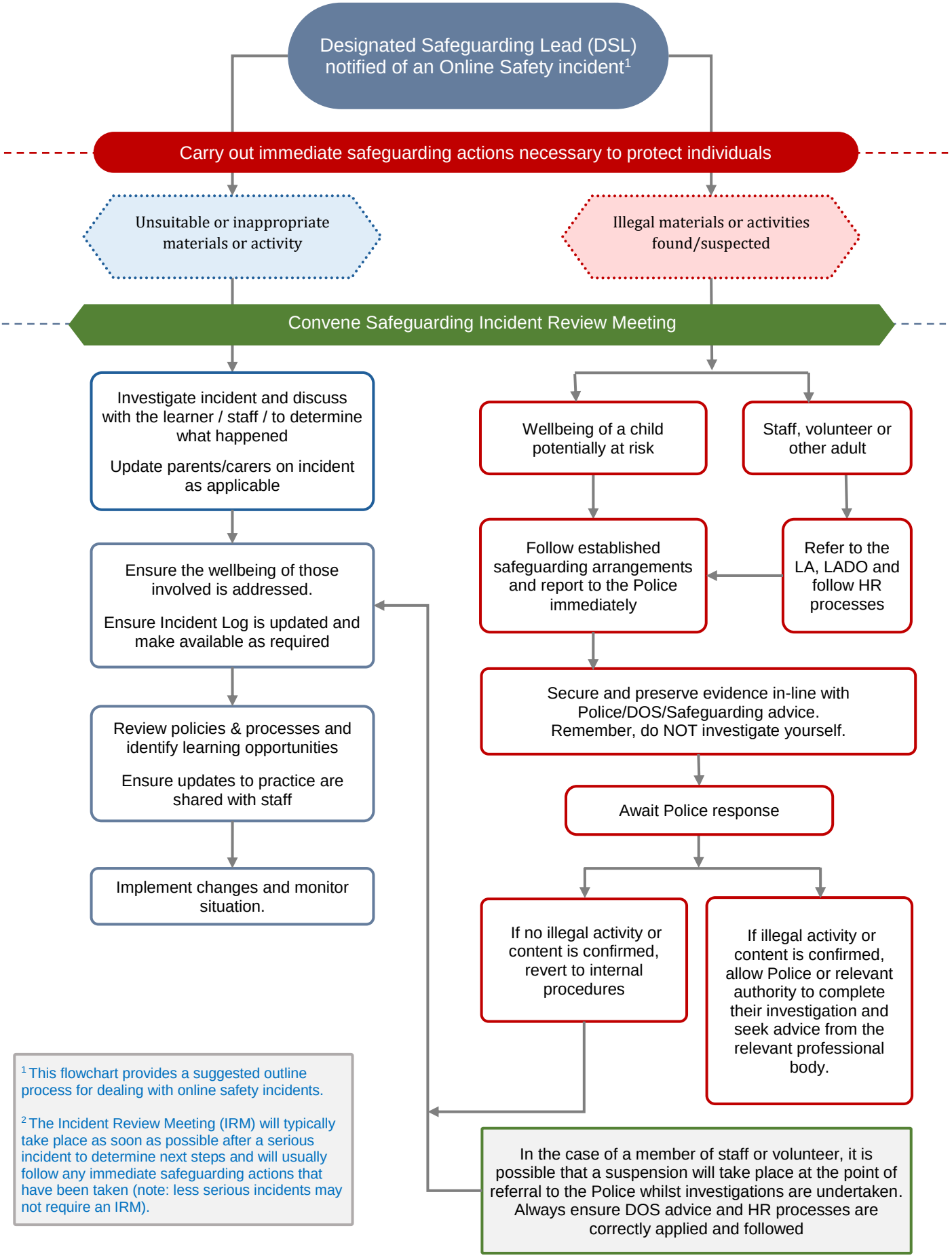
I have read and understand the above and agree to use the school digital technology systems (both in and out of the school) and my own devices (when agreed for use in school) within these guidelines.

Volunteer Name: .....

Signed: .....

Date: .....

Appendix E: Responding to incidents of misuse – flow chart



[1] This flowchart provides a suggested outline process for dealing with online safety incidents.

[2] The Incident Review Meeting (IRM) will typically take place as soon as possible after a serious incident to determine next steps and will usually follow any immediate safeguarding actions that have been taken (note: less serious incidents may not require an IRM).

Appendix F: 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 G: Template Reporting Log

Reporting Log

Group .....

Date	Time	Incident	Action taken		Incident Reported by	Signature
			What?	By whom?		

Appendix H: REPORT OF ONLINE SAFETY CONCERN

Child's Name:	
Date:	Time (hh:mm):
Reported By (full name):	Job Title:
Source of Concern: e.g. raised by parent. Seen in class, raised by another child	
Details of Concern (what was said, seen and/or done and by whom): *REMINDER: Behaviour concerns must also be reported directly to the class teacher*	
Staff action at time of concern being raised (including adults informed):	
Date and time passed to Online Safety Lead/ DSL/ Headteacher (Circle)	

Initial Follow Up Action Taken:		
By:	Job Title:	Date:
Further Follow Up Action Taken or Reason for no further action:		
By:	Job Title:	Date:

Appendix I: Staff Use of AI Acceptable Use Agreement

School Policy
Emerging technologies, including Artificial Intelligence (AI), are increasingly integrated into educational settings and the lives of staff and learners. These technologies have immense potential to enhance creativity, promote personalised learning, and improve operational efficiency. However, their use also presents risks that require clear policies and practices to ensure safety, security, and ethical application.

This acceptable use policy aims to ensure:

- Staff and volunteers are responsible users of AI and emerging technologies, prioritising safety and ethical considerations.
- School systems and users are protected from misuse or harm resulting from the use of AI.
- Staff have a clear understanding of their responsibilities when engaging with AI and emerging technologies in professional and personal contexts.

Acceptable Use Policy Agreement
I understand that I must use AI and emerging technologies responsibly to minimise the risk to the safety, privacy, or security of the school community and its systems. I acknowledge the potential of these 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 AI tools and technologies.
- I will only use AI tools and technologies for purposes authorised by the school and will ensure compliance with data protection laws (e.g. UK GDPR) when handling personal data.
- I will ensure that any sensitive or personally identifiable information about staff, students, or parents/carers is only entered into AI systems that have explicit approval and robust security measures in place.
- I will report any AI-related incidents or anomalies that could indicate misuse, bias, or harm to the appropriate person immediately.

In my communications and actions:

- I will respect copyright, intellectual property, and ethical standards when uploading content to prompt AI output.
- I will critically evaluate the outputs of AI systems to avoid spreading misinformation or biased content and will ensure that all AI-assisted decisions are made with appropriate human oversight.
- I will communicate professionally and responsibly when using AI systems.
- I will ensure transparency through appropriate attribution where AI has been used.

When engaging with learners:

- I will support learners on the safe, ethical, appropriate and effective use of AI.
- I will use AI tools to engage with learners in ways that uphold and enhance their privacy, wellbeing, and trust.

When using the school's systems and resources:

- I will use AI systems in compliance with established security measures and access protocols.
- I will ensure that any AI applications used in teaching or administration are vetted and comply with the school's policies.
- I will ensure generative AI tools are not used to impersonate others or create deceptive or harmful content.

When handling data:

- I will ensure compliance with the school's data protection policies when using AI for data analysis or reporting.
- I will ensure I have explicit authorisation when uploading sensitive school-related information into generative AI systems.

Responsibility and Accountability:

- I will use generative AI tools responsibly to create authentic and beneficial content, ensuring respect for individuals' identities and well-being.
- I understand that misuse of AI or emerging technologies could lead to disciplinary actions, including warnings, suspension, or referral to the appropriate authorities.
- I acknowledge that this agreement applies to all AI-related activities within and outside of school premises that are connected to my professional responsibilities.

Name: .....

Signed: .....

Date: .....

Appendix J: Effectiveness of Filtering and Monitoring - Annual Review Form

Filtering and monitoring effectiveness will be reviewed by the DSL and OSL at least annually, and following significant changes or incidents. Testfiltering (https://swgfl.org.uk/services/test-filtering/) will be used for this purpose, which will check that filtering is working appropriately on all internet-connected devices in all relevant locations. The results of these checks will be recorded in the table below:

Signatures					
Actions Taken					
Issues Identified					
Devices / Environments Tested					
Review carried out by:					
Date					

Appendix K: Technical Security Policy

(including Access, Device and Incident Management)

Purpose

This policy sets out how the school protects its technical infrastructure, systems and devices to ensure a secure and resilient digital environment. It supports safeguarding, data protection and business continuity and aligns with the DfE Technical Standards

Scope

This policy applies to:

- Staff, learners and governors
- Suppliers of third-party services and solutions
- School networks, servers and cloud systems
- School-owned devices
- User accounts and access controls
- Device configuration and management, including personal devices where permitted

Policy Statement

The school will ensure that its technical systems are managed in a way that:

- Protects users and data from unauthorised access or misuse
- Supports safe and reliable access to digital services
- Enables detection, response and recovery from technical incidents
- Is proportionate to risk and regularly reviewed

Access Control and Authentication

The school will ensure that:

- All users have unique accounts with appropriate access rights
- New user rights are allocated as part of induction
- Access is removed promptly when users leave the school
- Passwords and authentication methods reflect NCSC and DfE guidance
- Multi-factor authentication is used for sensitive systems where appropriate
- Administrator access is restricted and monitored
- System administrators and those with global/ confidential data system access use MFA to access systems.

System Security and Maintenance

The school will ensure that:

- Systems and software are licensed, supported and kept up to date
- Security patches are applied promptly
- Anti-virus and malware protection is in place across all systems
- Backups are taken regularly, stored securely (both locally and offsite, with rotation) and regularly tested
- Physical access to infrastructure is controlled

Device Management

The school will ensure that:

- Clear expectations exist for the use of school-owned and personal devices
- School devices are configured securely and managed appropriately, with regular/ automatic patches and updates
- Where personal devices are permitted, expectations are clearly defined and risk-assessed
- Acceptable Use Agreements reference responsible device use
- Users receive guidance on safe and appropriate device use

Supplier Management

The school will ensure that:

- Provision of third-party services and solutions are adequately contracted and regularly reviewed
- Suppliers can demonstrate adherence to school policy and alignment with the DfE Technical Standards

Incident Management
Technical incidents will be logged, escalated and reviewed. Serious incidents will be managed in line with safeguarding and business continuity procedures.

Review and Training
Technical security arrangements will be reviewed regularly. Staff with specific responsibilities will receive appropriate training, and users will be educated on their responsibilities.

Appendix L: Filtering and Monitoring Policy

Purpose

The purpose of this policy is to ensure that appropriate filtering and monitoring systems are in place to safeguard learners and staff from harmful or illegal online content, while enabling safe and effective teaching, learning and professional practice. Filtering and monitoring form part of the school's wider safeguarding responsibilities and are implemented in line with Keeping Children Safe in Education (KCSIE) and the DfE Filtering and Monitoring and Technical Standards.

Scope

This policy applies to:

- All users of the school's IT systems
- All school-owned devices
- Any device accessing the school's network or internet connection
- Filtering and monitoring provided through third-party or managed services

Roles and Responsibilities

- Governors provide strategic oversight and assurance that filtering and monitoring standards are met.
- Senior leaders ensure appropriate systems are in place, reviewed and resourced.
- The DSL leads safeguarding responses arising from filtering or monitoring alerts.
- The IT service provider maintains systems and provides reports as agreed.
- All staff report concerns relating to access, alerts or system effectiveness.

Policy Statement

The school will ensure that:

- Internet access is filtered to block illegal, harmful and inappropriate content
- Monitoring systems are in place to identify safeguarding concerns and enable timely intervention
- Filtering and monitoring are proportionate, transparent and risk-based
- Roles and responsibilities are clearly defined and understood
- Provision is reviewed regularly and improved in response to risk, practice and guidance

Filtering and monitoring are recognised as supporting safeguarding, not replacing education, supervision or professional judgement.

Filtering

The school will ensure that filtering systems:

- Block access to illegal content, including child sexual abuse material, terrorist material and other unlawful content
- Manage inappropriate and/or harmful content (including search terms and results). These may include:
    - Gambling
    - Hate speech/discrimination
    - Harmful content
    - Mis/Disinformation
    - Piracy and copyright theft
    - Pornography
    - Self-harm and eating disorders
    - Violence against women and girls
- Are age-appropriate and suitable for an educational environment
- Are applied consistently to all users, devices and internet connections, including backup connections
- Allow the identification of individual users and devices in the event of breaches of the filtering policy
- No user should be able to deactivate or bypass systems that filter illegal content.
- Prevent circumvention through VPNs, proxy services or similar technologies
- Support differentiated access for different user groups (e.g. staff and learners)
- Are reviewed regularly to avoid inappropriate over-blocking that may restrict teaching and learning

The school understands the capabilities and limitations of the system and potential impact on implementation and policy is understood.

The school will use recognised tools and guidance to assure the effectiveness of filtering provision e.g., testfiltering.com.

Monitoring

The school will ensure that monitoring:

- Enables the identification of safeguarding concerns in a timely manner
- Uses a combination of physical supervision, manual checks and technical systems as appropriate
- Generates alerts that can be prioritised and acted upon by trained staff
- Is subject to human review and professional judgement
- Is clearly communicated to users through policy and acceptable use agreements

Monitoring should be proportionate to the school's risk profile and should not create a culture of surveillance.

Review and Training

Filtering and monitoring provision should be reviewed at least annually and whenever risks or technologies change. Staff, governors and those with specific responsibilities will receive appropriate training.

Appendix M: Cyber Security Policy

Purpose
This policy sets out how the school prevents, detects, responds to and recovers from cyber threats. It supports the school's duty of care to protect users and data and aligns with the DfE Cyber Security Standards, National Cyber Security Centre (NCSC) guidance and NCSC Cyber Essentials

Scope
This policy applies to:

- Cyber threats including phishing, ransomware, malware and unauthorised access
- Staff, learners and governors
- Suppliers of third-party services and solutions
- Technical systems and cloud services
- Incident response and business continuity

Policy Statement
The school will take a proactive, risk-based approach to cyber security to:

- Reduce the likelihood and impact of cyber incidents
- Ensure timely and effective response to threats
- Build awareness and resilience across the school community

Cyber Security Strategy
The school will maintain a cyber security strategy that:

- Is supported by senior leaders and governors
- Is informed by risk assessment and incident learning
- Is reviewed regularly in line with emerging threats
- Is inclusive of all services and solutions, including those from third-party suppliers

Supplier Management
The school will ensure that suppliers:

- Can demonstrate adherence to school policy and alignment with the DfE Cyber Security Standards
- Are familiar with school incident response plan and able to respond effectively

Awareness and Education
The school will ensure that:

- Staff receive regular cyber awareness training
- Learners receive age-appropriate education on cyber risks
- Governors understand their oversight responsibilities

Incident Response
The school will maintain a clear cyber incident response plan that:

- Defines roles and escalation routes
- Supported by an effective communications strategy
- Supports safeguarding and business continuity
- Is tested periodically through simulations or exercises
- Ensures incidents are recorded and reviewed

External Assurance
Where appropriate, the school will engage external expertise to assess cyber resilience and will work towards recognised standards or certifications.

Review
Cyber security arrangements will be reviewed annually, or sooner if required by incidents, guidance or changes in technology. Lessons learned from managing incidents should inform improvements to the strategy.

Appendix N: Public Online Communications Policy

Purpose
The purpose of this policy is to set out how the school manages public online communications in order to reduce risk, promote safeguarding and online safety, celebrate success and communicate effectively with the wider school community.

Public online communications include the school website, newsletters, learning platforms, public messaging systems and official social media accounts.

This policy supports the Online Safety, Filtering and Monitoring, Technical Security, Cyber Security, Information Management and Data Protection (including Data Security) policies and reflects Keeping Children Safe in Education (KCSIE), UKSIC guidance Best Practices for Managing Images and Videos on School Websites, DfE statutory publication requirements (Maintained schools) and (Academies).

Scope
This policy applies to:

- All staff and governors
- All public online communications representing the school
- Official school accounts and platforms
- Personal accounts where they directly reference or represent the school
- School content published at any time, from any location or online platform

Policy Statement
The school will ensure that:

- Public online communications are accurate, lawful and appropriate
- Safeguarding considerations are prioritised
- Personal data is protected in line with the Information Management and Data Protection (including Data Security) Policies
- Images and video are published only in line with consent procedures
- Copyright and intellectual property are respected
- Communications reflect professional standards
- Public references to the school are monitored appropriately

Roles and Responsibilities

- Governors provide strategic oversight and ensure compliance with statutory publication requirements.
- Senior leaders approve official accounts and oversee monitoring and moderation processes.
- Account administrators maintain secure access, monitor content regularly and ensure policy compliance.
- All staff must follow this policy, maintain professional standards and report concerns.

Creation of Public Online Accounts

- New public online accounts may only be created following approval by senior leadership.
- Proposals must define purpose, audience, responsible staff members and monitoring arrangements.
- At least two authorised staff members must have access to any official public account.

Monitoring and Moderation
The school will ensure that:

- Public communications are monitored regularly
- Comments are reviewed and moderated appropriately
- Harmful or inappropriate content is removed
- Serious incidents are recorded and escalated where necessary

Professional Standards
All public communications must:

- Be respectful and professional
- Avoid discriminatory, offensive or defamatory content
- Protect confidentiality
- Avoid internal grievance discussions
- Avoid disclosure of sensitive information

Use of Images and Media
The school will ensure that:

- Appropriate consent is obtained
- Images are appropriate and dignified
- Learners are not identified unnecessarily
- Images are removed where consent is withdrawn
- To reduce the risk of illegal manipulation of publicly available images of staff and learners, the school has procedures in place to control how those images are shared online. (n.b., UKSIC guidance Best Practices for Managing Images and Videos on School Websites)

Personal Use and Association with the School
Staff may use personal social media accounts; however:

- Where referencing the school, appropriate disclaimers must be used
- Personal use must not impact professional standards nor school reputation
- Staff must not engage with current learners via personal accounts
- Excessive or inappropriate use during working hours may result in disciplinary action

Handling Complaints and Abuse
Where negative comments are made online:

- The school will respond proportionately
- Abusive content should be challenged and removed
- Parents'/carers' complaints should be directed to formal complaints procedures
- Serious matters may be escalated to senior leaders or external agencies

Training and Awareness
The school will ensure that:

- Staff responsible for public accounts receive guidance and training
- Governors understand oversight responsibilities
- The wider community is informed of expected standards

Review and Continuous Improvement
This policy will be reviewed annually and updated in response to legislative changes, national guidance or emerging risks.