Policy Name	**ONLINE SAFETY**
Relevant To	**Federation ☒** **Bidwell Brook Only ☐** **Ellen Tinkham Only ☐**
Type of Policy	**Model ☐** **School ☒**
Name of Policy Holder	**Kate Bromage**
Subject/Department	**Online Safety Committee**
Approved By	**Full Governing Body ☒** **CBT Governors ☐** **T&L Governors ☐** **SLT ☐**
Version Date (if applicable)	**n/a**
Date of Last Review	**Autumn Term 2026**
Date of Next Review	**Autumn Term 2027**

CONTENTS

1. Scope of the Online Safety Policy 3
2. Policy Development, Monitoring and Review 3
3. Policy and Leadership 3
4. Online Safety Policy 6
    - Acceptable Use 7
    - Reporting and Responding 11
    - Responding to Learner Actions 14
    - Responding to Staff Actions 15
    - Use of Artificial Intelligence (AI) 16
5. Education 17
    - Online Safety Education Programme 17
    - Staff 18
    - Governors 18
    - External Stakeholders 18
    - Working with Parents & Carers 19
6. Technology 19
    - Filtering and Monitoring 19
    - Technical Security 20
    - Cyber Security 20
    - Data Protection 20
7. Technology Practice 20
    - Device Management 21
    - Digital Content 21
    - Public Online Communications 22
    - Outcomes 22

Appendix 1 - Bring Your Own Device – Acceptable Use 23
- Appendix 1.1 BYOD Permission Form for Key Stage 3 and Under 25
- Appendix 1.2 BYOD Permission Form for Key Stage 4 and Under 26
- Appendix 1.3 BYOD Permission Form for Key Stage 5 28

Appendix 2 - ICT Acceptable Use and ICT Code of Conduct 30
Appendix 3 – Computer Misuse and Cyber Choices 33
Appendix 4 – Filtering and Monitoring 35
Appendix 5 – Technical Security 38
Appendix 6 – Cyber Security 40
Appendix 7 - Electronic Devices: Searching, Screening and Confiscation 42
Appendix 8 – Public Online Communications 45
Links to organisations or documents 48

1. SCOPE OF THE ONLINE SAFETY POLICY

This Online Safety policy sets out how the Learn to Live Federation 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 Learn to Live Federation community who access or use Federation digital systems including staff, pupils and Governors. Its principles also apply to the use of personal devices by learners on the school site (where permitted).

Where online safety concerns or incidents occur outside school and are known to the school, the Learn to Live Federation will respond in line with this policy and related procedures, including the Federation's Safeguarding and Behaviour policies. Where appropriate, parents & carers will be informed of incidents involving inappropriate online behaviour that take place out of school.

2. POLICY DEVELOPMENT, MONITORING AND REVIEW

This policy has been developed by the Online Safety Committee, drawing on the expertise and responsibilities across the Federation. Current membership includes:

- Senior Leaders
- Designated Safeguarding Lead (DSL) / Online Safety Lead (OSL)
- Teaching & Learning Online Safety Lead
- Support Staff (including ICT)

Escalation following Serious Incidents

The school will inform relevant external agencies as appropriate eg LADO and the Police.

Monitoring the Impact of the Policy

The Federation will evaluate the effectiveness of this policy using evidence such as CPOMS, reviews of the effectiveness of the filtering systems, Internal network activity monitoring data, surveys where applicable.

3. POLICY AND LEADERSHIP

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.

Executive Head and Senior Leaders
Senior Leaders set the culture and ensure that systems are effective. In line with Keeping Children Safe in Education (KCSiE), each site DSL holds day-to-day lead responsibility. Senior leaders will:

- Ensure the school meets its safeguarding duty of care, including online safety;
- Know and apply procedures for serious allegations involving staff (Executive Head plus the Federation HR Manager);
- Ensure that the DSL/OSL, ICT team and relevant colleagues are trained and able to fulfil their roles;
- 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 are 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 regular online safety reports and act on emerging risks and themes;
- Ensure the Federation Finance Manager works alongside the DSL/OSL and with the ICT team on an annual basis, to review of the effectiveness on filtering and monitoring systems and ensure that these are recorded.

Governors

Governors to approve the Online Safety Policy and challenge its effectiveness. KCSiE requires them 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 be taught about safeguarding, including in relation to online safety;
- Review the DfE Filtering and Monitoring Standards and discuss with the Federation ICT Manager what more needs to be done to support the Federation in meeting this standard.

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

- Meet regularly with the DSL/OSL;
- Receive an Online Safety report plus, if relevant, any anonymised incidents and monitoring summaries from CPOMS via termly Head's Reports;
- Check delivery of key commitments eg education, reporting, staff training;
- Have an understanding of filtering and monitoring and through regular review, assess the effectiveness of filtering and monitoring with the OSL and Federation ICT Manager in line with KCSiE and DfE Filtering and Monitoring standards;
- Report to the relevant governor committee: Core Business Team (policy approval at Full Governors);
- Undertake basic cyber security awareness training and support school cyber security oversight;
- Governors also support parent & carer and community engagement in online safety.

Designated Safeguarding Lead (DSL) / Online Safety Lead (OSL)

KCSiE (Para 125) states the DSL leads safeguarding and child protection, including online safety, and understands filtering and monitoring systems and processes. The DSL will:

- Lead safeguarding, including online safety, with clear responsibilities in their job description (KCSiE 2026 guidance);
- Maintain up-to-date knowledge of online risks, filtering/monitoring and cyber security;
- Co-ordinate and record online safety concerns and incidents, escalating and referring in line with safeguarding procedures;
- Liaise with SLT, the Online Safety Governor, the Federation ICT Manager and relevant external partners as required;
- Review anonymised incident patterns and filtering/monitoring information;
- With the Federation ICT Manager, carry out an annual review of the effectiveness on filtering and monitoring systems and ensure that these are recorded;
- Report regularly to SLT and drive continuous improvement across relevant policies and practice, using evidence including incident data, monitoring information, audits and Federation self-review processes;
- Ensure appropriate support for learners with SEND.

In their role as Online Safety Lead, the OSL will:

- Lead the Online Safety Group and support the DSL day to day;
- Lead development and review of online safety documentation;
- Co-ordinate awareness, staff confidence and reporting readiness through appropriate training;
- Work with curriculum leads to map, embed and evaluate online safety education;
- Liaise with ICT and pastoral/support teams;
- Maintain current knowledge of risks across content, contact, conduct and commerce.

Online Safety Curriculum Lead (Teaching & Learning)

The Curriculum Lead will work with other Subject Leads and the DSL/OSL to deliver a planned Federation-wide online safety programme through appropriate channels, eg PSHE/RSE, other curriculum areas, assemblies/pastoral provision and national initiatives eg 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 have signed the ICT Code of Conduct;
- Maintain professional boundaries (including online/remote learning);
- Supervise learner use of technology and follow procedures for online safety issues;
- Embed online safety where appropriate; teach research skills, copyright and plagiarism awareness;
- Challenge harmful online behaviour and report concerns promptly;
- 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 / annual training, with updates as needed; contribute to improvement by sharing learning and concerns.

Federation ICT Manager and ICT Support Team

The Federation ICT Manager and ICT Team supports leaders and the DSL to meet DfE filtering, monitoring and technical standards. Where services are outsourced, the school remains accountable. The Federation ICT Manager and ICT Team 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;
- Monitor systems for misuse and report concerns promptly to the Federation Finance Manager;
- Follow the Federation's Online Safety Policy and security procedures, and keep technical knowledge current.

Learners

Learners will:

- Follow the Bring Your Own Device agreements, where relevant;
- Report concerns and know how to get help;
- Use technology responsibly, respecting others and their copyright and intellectual property;

- Use AI responsibly: protect original work, check accuracy and avoid plagiarism;
- Understand that out-of-school behaviour may be addressed where it affects the school community.

Parents & Carers

Parents & carers are key partners in reinforcing safe online behaviour. The school will:

- Publish the Federation Online Safety Policy;
- Provide guidance on the responsible use of online technologies and seek permissions for digital services/images where required;
- Share updates through meetings, newsletters, online channels and campaigns.

Parents & carers will be encouraged to reinforce key messages and support safe use of personal devices, where relevant.

Online Safety Committee

The Online Safety Committee provides strategic oversight of online safety, monitors implementation and impact of the Federation Online Safety Policy, and ensures online safety is embedded across safeguarding, curriculum and technical practice. Core responsibilities include:

- To draft, review and monitor the Federation Online Safety Policy and related documents;
- Oversee filtering and monitoring, including requests for change;
- Map and review online safety education for breadth, progression and relevance;
- Review anonymised incident data and technical logs to identify trends and emerging risks;
- Gather feedback from learners, staff and parents & carers and turn this into improvement actions;
- Promote learner voice, peer support and awareness activity;
- Track and evidence improvement actions through the Federation's quality assurance and self-review processes.

Governance and Impact

- Operates to agreed Terms of Reference (membership, frequency, reporting lines), reviewed annually;
- Co-ordinates with Safeguarding, Behaviour, Curriculum and Learner Voice as needed;
- Reports key themes, actions and impact to SLT and Governors, and shares appropriate summaries with the wider community.

4. ONLINE SAFETY POLICY

The Online Safety Policy is part of the Federation safeguarding framework and should be read alongside Safeguarding & Child Protection, Behaviour and Data Protection policies.

What the policy does

- Defines responsibilities for online safety;
- Sets expectations for safe, professional and ethical use of technology (including AI);
- Sets out reporting, recording and response procedures for online safety incidents;
- Supports compliance with KCSiE, DfE Technical Standards and UK GDPR;
- Promotes learners' digital competence and critical understanding.

Implementation, monitoring and review

- Developed through the Online Safety Group and reviewed at least annually (KCSiE Para 121), and sooner if risks/technology change;

- Monitored by the DSL/OSL and Governors using anonymised incident trends, filtering/monitoring reports and education review activity (eg the Federation's online safety self-review process safe, the Federation's online safety curriculum);
- Findings inform improvement planning and staff training priorities.

Communication and accessibility

- Shared at staff induction and reinforced through training;
- Communicated to learners and parents & carers through Acceptable Use documentation and awareness activity;
- Published on the school website.

Acceptable Use

Acceptable use is defined through the Federation Online Safety Policy and Acceptable Use documentation. Acceptable Use documents matter most when they are understood, reinforced and followed - not simply signed.

Reinforcement

- Staff handbook;
- Reminder emails from the Federation ICT Manager;
- Posters in Reception / areas where technology is used ie ICT suites;
- Curriculum and awareness sessions;
- Communications with parents & carers;
- School website.

Acceptable/Unacceptable Actions

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 • 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
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 (eg personal/financial data, databases, access codes) • Disabling, impairing or disrupting network/services (eg 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

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable & illegal
Un-acceptable (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 Acceptable Use documentation)				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 (eg 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	
	Sharing content that is offensive, undermines the school's ethos, breaches integrity, or brings the school into disrepute				X	

Activities during school hours - non-educational purposes	Staff and other adults on personal devices (not school devices)				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 (eg Roblox, Fortnite, Minecraft)			X		X			
Online shopping and digital commerce (including in-app purchases, marketplaces, subscriptions)			X		X			

Cloud storage and file sharing (eg Google Drive, OneDrive, Dropbox, WeTransfer; P2P/torrents)			X		X	
Social media and user-generated platforms (eg TikTok, Instagram, Snapchat, X, Reddit) and other age-restricted services eg within the Online Safety curriculum			X			X (KS4+ in lessons)
Messaging, chat and voice (eg WhatsApp, iMessage, Snapchat, Discord, Teams personal accounts)			X			X (KS4+ in lessons)
Streaming entertainment/media (video, music, podcasts) eg Netflix, Disney+, Spotify			X		X	
Video platforms and livestreaming (eg YouTube, Twitch, TikTok LIVE, Instagram Live)			X			X (KS4+ in lessons)
Personal mobile phones and smart devices on site (phones, smartwatches, earbuds) eg staff to access iTrent, CPOMS login. eg Sixth Form learners during "common room time"			X	X (MFA/ CPOMS)	X	X (6th Form only)
Taking photos/video/audio on devices (including sharing, location data and consent)	X				X	
Other personal devices (eg, tablets, handheld consoles, VR headsets, wearables)			X			X (KS4+ in lessons)
Personal email accounts on site or on the school network/Wi-Fi (eg Gmail, Outlook.com)			X		X	
School email used for personal communication (non-work/non-learning)	X				X	
Unapproved AI tools/services (generative AI chatbots and image/video tools, AI companions, browser extensions)			X		X	

Reporting and Responding

Introduction

The Federation 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 Federation 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 Federation 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 Federation 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 states that staff should have a professional curiosity and speak to their Designated Safeguarding Lead (or a Deputy Designated Safeguarding Lead) if they have concerns about a child.

Reporting Concerns

The Federation will ensure that:

- Clear, accessible reporting routes are in place for all members of the school community including pupils, staff, Governors, parents & carers and visitors;
- Reporting processes are fully aligned with safeguarding procedures, including the child protection, whistleblowing, managing allegations and complaints policies;
- Reporting options are available such as speaking with the Designated Safeguarding Lead (DSL) or online via CPOMS;
- Reporting routes are well publicised through induction, assemblies and Whole School Meetings, 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 Federation will ensure that:

- Reports are acknowledged and responded to promptly, considering the safety and wellbeing of the person reporting;
- The DSL / Online Safety Lead, Senior Leaders and the Federation ICT Manager 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;

- 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 Federation 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 termly reports)
    - Staff
    - Learners, where appropriate
    - Parents & carers through general communications

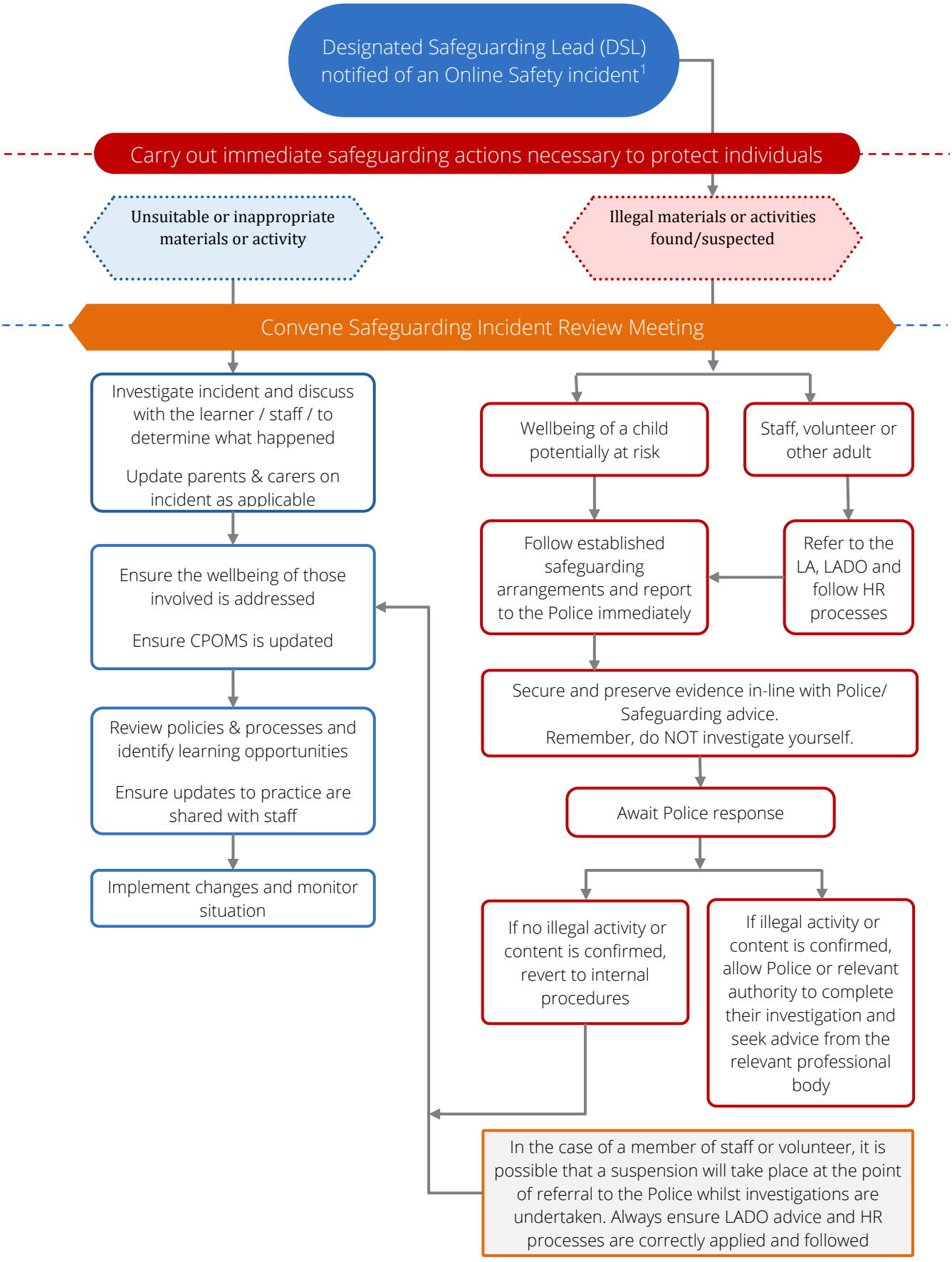
External Support and Escalation

The Federation will work with appropriate external agencies when required, including:

- LADO;
- Police / CEOP;
- UK Safer Internet Centre's Professionals Online Safety Helpline.

Reporting Harmful Content Service

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


Designated Safeguarding Lead (DSL) notified of an Online Safety incident[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 CPOMS is updated
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/ 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 LADO advice and HR processes are correctly applied and followed

The Federation will 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 Social Worker	Refer to Federation ICT Manager	Inform parents & carers	Remove device / network / internet / access rights	Refer to Police
Accessing illegal material (or attempting to), as defined in the earlier "Unsuitable/Inappropriate Activities" section.	X	X	X	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	X	X	
Unauthorised downloading/uploading, file sharing or distribution of files.	X	X		X			
Bypassing filtering (eg proxy sites, VPNs or similar tools).	X	X		X			
Failing to report accidental access to offensive or pornographic material	X	X		X	X		
Deliberately accessing offensive or pornographic material (or attempting to)	X	X	X	X	X	X	X
Sharing or receiving content that breaches copyright or data protection law.	X	X		X	X		

Unauthorised use of devices, including taking photos/videos or audio recordings and using a smartphone in school	X	X	X	X	X	X	
Any online behaviour that could bring the school into disrepute or undermines the school's ethos.	X	X		X	X	X	
Repeated breaches of these rules following previous warnings or sanctions.	X	X	X	X	X	X	

Responding to Staff Actions

Incidents	Refer to line manager	Refer to Federation ICT Manager	Refer to SLT / Executive Head	Refer to LADO	Professional Conversation / Issue a warning	Further Disciplinary action in line with Staff Code of Conduct
Accessing illegal material (or attempting to), as defined in the earlier "Unsuitable/Inappropriate Activities" section.	X	X	X	X	X	X
Breaching data protection or cyber-security requirements, including network security rules.	X	X	X		X	
Accessing offensive or pornographic material (or attempting to).	X	X	X	X	X	X
Damaging systems or data, including corrupting/deleting others' data or deliberately damaging hardware/software.	X	X	X		X	
Bypassing filtering controls (eg proxy sites, VPNs or similar methods).	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		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	X	X

Use of personal email/social media/messaging to communicate with learners.	X	X	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	X		X	
Mishandling personal data, including storing, displaying or transferring it insecurely.	X	X	X		X	
Any action that undermines professional conduct or a staff member's professional standing.	X	X	X		X	
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.	X	X	X		X	
Failing to report incidents, whether accidental or deliberate.	X	X	X		X	
Repeated breaches following previous warnings or sanctions.	X	X	X	X	X	X

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 by using Federation approved AI platforms - Microsoft Co-Pilot, SLT AI and Teachmate. 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.

The Federation 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.

With regards the safe use of AI, data protection and security, the Federation 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. AI platforms used must meet data protection and security requirements;
- Approve tools and accounts. Only Federation-approved AI platforms may be used and staff should use school-provided AI accounts where available to support oversight and reduce risk;
- Safeguard sensitive information. Sensitive materials including pupil data must not be entered into AI platforms.

In terms of quality, fairness and integrity, the Federation 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 (eg documents, presentations, communications), staff should make this clear where appropriate;
- Address bias and discrimination. We recognise AI outputs may reflect bias. The Federation will use appropriate safeguards, review processes and procurement checks to prioritise fairness and safety;
- Protect copyright and intellectual property. The Federation 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.

For reporting, monitoring and accountability, the Federation will:

- Require prompt reporting of AI-related concerns including misuse, data incidents or inappropriate outputs, via CPOMS ensuring the Federation ICT Manager is tagged;
- Maintain an up-to-date Data Protection Impact Assessment of AI platforms in use, with purposes and risks recorded;
- Provide parents & carers with clear information about how AI is used in school via the Federation AI Policy on the school website.

Any improper use of AI platforms including breaches of this policy, data protection failures, misuse of sensitive information, or failure to follow agreed processes, may result in action under the Federation's Disciplinary Policy.

5. EDUCATION

Online Safety Education Programme

Online safety education is a core part of the Federation'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 Federation delivers a planned, 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", and resources such as the Federation Curriculum Policy. Learning is age-appropriate, builds on prior learning, is matched to need and is taught through existing curriculum areas (including RSHE/RSE and Health education), with assessment and clear intended outcomes.

The programme develops learners' ability to:

- 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 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).

Where internet use is planned, learners are guided to appropriate resources and supported if unsuitable content is encountered. Filtering may be temporarily adjusted for legitimate curriculum research, with auditable approval and clear rationale.

Learner voice is actively used to strengthen the school's approach through feedback and learner representation (eg Student Council), and opportunities such as online safety activities.

Staff

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 Federation'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 documentation 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 eg via SWGfL;
- 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 and awareness activity. This is particularly important for governors serving on committees with responsibility for safeguarding, online safety, technology or health and safety. Training and updates may be provided through participation in school training and information sessions. Governors will also receive regular updates from the DSL / OSL to review key themes, incidents and current priorities. Enhanced training will be provided for (at least) the Online Safety Governor. This will include:

- Basic cyber security awareness training;
- Training to understand the Federation's filtering and monitoring provision, enabling effective participation in required checks and reviews.

External Stakeholders

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

The following principles underpin the Federation's engagement with external stakeholders:

Working with Parents & Carers

The Federation will support parents & carers to understand online risks, build confidence and reinforce safe online behaviours at home. This includes regular communication and awareness-raising about online safety issues, curriculum content, and reporting routes; providing information through newsletters and the school website; offering opportunities such as parent & carer workshops, information events, or drop-ins focused on online safety. We encourage learners in sharing online safety messages with parents & carers, including contributing to information events.

Parents & carers are regularly signposted to trusted national resources (eg UK Safer Internet Centre, Internet Matters, Childnet). The Federation also promotes and participates in key national events such as Safer Internet Day.

6. TECHNOLOGY

Purpose

The Federation 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.

Filtering and Monitoring

The Federation 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. (eg DfE Technical Standards, DfE Generative AI: product safety standards; KCSiE) and best practice guidance (eg UKSIC Appropriate Filtering and Monitoring). The Federation ICT Manager 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 Federation 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;
- monitoring supports the rapid identification of safeguarding concerns and enables timely intervention;
- 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.

Oversight and Review

The DSL / OSL, Federation ICT Manager, technical staff and Governors have clear roles and responsibilities:

- Governors will review the DfE Filtering and Monitoring Standards and discuss with the Federation ICT Manager 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. Reviews will be carried out by the Federation Finance Manager, in their capacity as line manager to the Federation ICT Manager, with the support of the DSL/OSL and ICT support. 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;
- CPOMS reports provide actionable information for safeguarding decisions;
- no system is relied upon in isolation; reporting routes and professional judgement remain central.

Technical Security

The Federation takes steps to ensure that its technical infrastructure is secure, reliable and well managed and meets its statutory requirements. The Federation ensures that:

- access to systems and data is controlled through appropriate authentication and permissions;
- devices, networks and systems are protected through secure configuration, patching and malware protection;
- 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;
- responsibilities for technical security are clearly defined and supported by appropriate expertise;
- systems are regularly reviewed and tested, meet statutory requirements and address emerging threats.

Cyber Security

The Federation 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 Federation 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.

Data Protection

The Federation is committed to protecting personal data and complying with data protection legislation. The Federation ensures that:

- personal data is processed lawfully, fairly and transparently;
- a Data Protection Officer (DPO) is appointed and appropriate governance arrangements are in place;
- 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 platforms are in use, human oversight will be maintained for significant decisions, risk assessments will be conducted and the Federation will ensure automated systems are transparent and explainable.

Review

Arrangements for filtering, monitoring, technical/cyber security and data protection are reviewed regularly and updated to reflect changes in technology, emerging safeguarding risks and national guidance and statutory expectations.

7. TECHNOLOGY PRACTICE

Purpose

The Federation 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.

Device Management

The Federation manages the use of digital devices in a way that supports safeguarding, learning and responsible behaviour. This reflects KCSiE's requirement for clear guidance on the use of devices and explicitly links device use to behaviour, safeguarding and education.

The Federation ensures that:

- expectations for the use of school-owned and personal devices are clearly defined and communicated;
- device use is consistent with safeguarding, behaviour and data protection policies and acceptable use documentation;
- appropriate technical and procedural controls are in place to support safe use;
- staff and learners 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.

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

Digital Content

The Federation 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 Federation 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.

Public Online Communications

The Federation 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 Federation 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;
- 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.

Review

Technology practice is reviewed regularly to reflect changes in technology and online behaviour; emerging safeguarding risks; feedback from staff, learners and parents & carers and national guidance and statutory expectations.

Outcomes

The impact of the Federation Online Safety Policy and practice is evaluated regularly using evidence such as online safety incident reports via CPOMS, behaviour and bullying records via CPOMS 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 Federation's assessment and monitoring processes to evaluate learners' online safety knowledge, behaviours and understanding. 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.

APPENDIX 1

BRING YOUR OWN DEVICE AGREEMENT - ACCEPTABLE USE

TO BE READ IN CONJUNCTION WITH THE FEDERATION'S ONLINE SAFETY POLICY

This agreement provides the rules of behaviour for the use of personally owned tablets, smartphones and any other personal device (including any device with internet access capability) by pupils of the Learn to Live Federation.

- The Learn to Live Federation accepts no responsibility and cannot be held liable for the loss or damage to any pupil's personal mobile device. Costs of replacement or repair due to loss or breakages (accidental or not) will be met by the parents & carers;
- It is the responsibility of the parents & carers to ensure that any personal mobile device conforms to the requirements of the school;
- It is the responsibility of the parents & carers to ensure that any personal mobile device is fit for purpose, safe, clean and virus free;
- It should be maintained to an acceptable standard with all relevant operating system patches, security updates and suitable antivirus software installed;
- The device must be free of illicit or unsuitable material. Any personal mobile device found to have health and safety defects should not be brought to school. Images of students or staff which are held on a personal mobile device are to be deemed personal data and covered by the Data Protection Act;
- Under no circumstances is this data to be distributed without prior written consent from the school. Furthermore, no images or video data which has been recorded at the school can be transmitted or uploaded to the internet at any time without the school's written permission;
- Personal mobile devices may not be used to record, transmit or upload images or video data of other pupils or teachers;
- The pupil's parents & carers are required to read, sign and submit the Bring Your Own Device Agreement to the school. Where applicable, Key Stage 4 and Key Stage 5 students are also required to read, sign and submit their agreement to the school;
- The use of personal mobile devices whilst at school is generally prohibited and should primarily be for education and communication only. Permission must be obtained from the school before using such devices for personal use under supervised conditions;
- The Learn to Live Federation reserves the right to withdraw from any agreement and refuse to allow the use of mobile devices by individual students at any time;
- The Federation reserves the right to amend the Bring Your Own Device Agreement at any time and in keeping with the Online Safety Policy.

KEY STAGE 4 STUDENTS AND ABOVE

For Parents & Carers

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

The Learn to Live Federation wishes to ensure:

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

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

Use of SIM Enabled Mobile Devices for Students in Key Stage 4 & 5 only

The Learn to Live Federation is committed to safeguarding and promoting the welfare of children and young people. This includes safeguarding them from risks associated with mobile technologies and the internet. We are aware that young people are continuously exposed to an increasing range of risks, whether they are using mobile phones, iPads or games consoles to access online gaming, social media, chatrooms or websites.

One way to support our young people is to allow them to use their mobile devices in a controlled environment and provide them with a thorough, practical education which empowers them to take control and enables them to recognise the dangers in order to avoid them. Below is an outline of what this will look like for your young person. It will inform you of precautions in place to safeguard our students as well as the responsibilities you will have under this agreement.

Your young person will attend a series of online safety sessions and must have understood and sign their own agreement prior to being allowed access to their mobile phone or other device whilst in school. Your young person will only have access to their mobile device when needed for educational purposes or at agreed times during the day. For Sixth Form students only, this will include usage of their mobile device at lunchtime.

The device may only be used in agreed locations either within the school or when off-site. Your young person will be supervised by a member of staff at all times who may ask to see the mobile device or the activities being undertaken by the young person at any time. There will be no access to the school's wi-fi. This means that if a student wishes to access the internet, they will do so using their own mobile network connection which will be unfiltered.

If your young person is found to be accessing inappropriate materials (including but not limited to using/ accessing strong language or accessing indecent images) or taking part in activities which could pose a danger to themselves or others (including but not limited to sharing personal information, engaging in exchanges with unknown people or taking part in online bullying), they will no longer be able to use their mobile device at school and you will be informed. In these instances, the mobile device will be confiscated and you will be required to collect the device on your young person's behalf.

Your young person will not be allowed to take photographs or videos of staff or other students while using their mobile devices. Please be aware that if you allow your young person to use their mobile device at Bidwell Brook School or Ellen Tinkham School, and in the vicinity of other students using their mobile devices, they may have access to all activities available on their device and online. These include making phone calls, sending text messages, accessing social media, watching online videos, communication sites and chat rooms and playing online games.

If there are any breaches of these protocols, you will be responsible for correcting these. For example, if a photo or video has been taken of another student, it will be your responsibility to ensure that these are deleted permanently. Equally, if your young person has posted something online and the school asks you to remove it, you will be responsible for doing so.

APPENDIX 1.1

PERMISSION FORM FOR STUDENTS IN KEY STAGE 3 AND BELOW
Parent / Carer to read and complete

It is prohibited for pupils in Key Stage 3 and below to have access to any personal device, other than a mobile device specifically for learning, during school hours. Any devices brought into school will be held in a secure location and not accessed during the day.

If bringing a mobile device into school to be used for educational purposes during school hours eg an AAC device to support a child's learning

- Access to the Federation's wireless network entails personal responsibility and compliance with all school rules. Access to the Federation's wireless network will be at the discretion of the school based on the requirements for access.
- Internet access in school must only be via the school's network. Any device with independent access to the internet (mobile phones or other devices with SIM cards) must not be used in school unless the SIM card is removed. Devices where the SIM card cannot be removed must not be used during the school day and will held in a secure location and not accessed.
- The school reserves the right at any time to monitor, inspect and if necessary confiscate any mobile device brought into school. Pupils will adhere to teacher and staff instructions regarding the use of mobile devices at all times especially when in class.
- The use of personal mobile devices must not be a disruption or a distraction to teachers or other pupils.

FOR PARENTS & CARERS IN KEY STAGE 3 AND BELOW:

- **I sign this form and confirm I have read and agree with the Federation's Online Safety Policy.**
- **I agree to allow my child to use their mobile device for the purposes outlined in Appendix 1.**

Student Name	
Parent / Carer Name	
Signature	
Date	

APPENDIX 1.2

PERMISSION FORM FOR STUDENTS IN KEY STAGE 4 ONLY

- **Parent / Carer to read and complete**
- **Student to read and complete**

It is prohibited for pupils in Key Stage 4 to have access to any personal device, other than a mobile device specifically for learning, during school hours. Any devices brought into school will be held in a secure location and not accessed during the day.

If bringing a mobile device into school to be used for educational purposes during school hours eg a mobile phone

At selected points across the year, and in line with their education, selected students in Key Stage 4 will use their own devices during ICT lessons to develop their knowledge and understanding of how to use social media platforms safely. They will also access learning opportunities to fully understand how to use their phone to safeguard themselves. These sessions will be carefully controlled and monitored by staff and parents & carers will be notified when these sessions are due to take place.

If bringing a mobile device into school to be used for educational purposes during school hours eg an AAC device to support a young person's learning

- Access to the Federation's wireless network entails personal responsibility and compliance with all school rules. Access to the Federation's wireless network will be at the discretion of the school based on the requirements for access.
- Internet access in school must only be via the school's network. Any device with independent access to the internet (mobile phones or other devices with SIM cards) must not be used in school without prior knowledge and permission of the Class Teacher. Unless the device is being used in a specific lesson, devices where the SIM card cannot be removed must not be used during the school day and will held in a secure location and not accessed.
- The school reserves the right at any time to monitor, inspect and if necessary confiscate any mobile device brought into school. Pupils will adhere to teacher and staff instructions regarding the use of mobile devices at all times especially when in class.
- The use of personal mobile devices must not be a disruption or a distraction to teachers or other pupils.

FOR PARENTS & CARERS IN KEY STAGE 4 ONLY:

- **I sign this form and confirm I have read and agree with the Federation's Online Safety Policy.**
- **I agree to allow my young person to use their mobile device for the purposes outlined in Appendix 1.**
- **I understand that every precaution will be taken by staff to ensure that my young person is safe whilst using their own mobile device but that the risks associated with using the internet or mobile devices is ever present.**

Student Name	
Parent / Carer Name	
Signature	
Date	
Make / Model of Device(s)	
Mobile Number (if applicable)	

FOR STUDENTS IN KEY STAGE 4 ONLY, PARTICIPATING IN ONLINE SAFETY LESSONS:

- **I understand I will take part in online safety lessons and know that I must keep my personal information safe.**
- **I know where I can get online safety help, if I need it.**
- **I understand that I must follow the rules set out below in order to use my own mobile device:**
    - **I will not take photographs or videos of other students or members of staff.**
    - **I must not create, upload or share any inappropriate messages or images, including swearing or comments about others.**
    - **I will not access inappropriate materials when I go online.**
    - **I will only text or call the people on the list approved by my parent /carer.**
    - **I will only access the sites and apps that are on the list approved by my parent /carer.**
    - **My phone/mobile device must be handed in at the start of the day.**
    - **I will only use my device in the specified location, at a time when I am advised.**
    - **I will allow staff to see what I am doing if they ask.**
    - **I will hand my phone/mobile device in at the end of the session and this can be collected at the end of the school day.**
    - **If I am found to be breaking any of these restrictions, I will not be allowed to use my mobile device on site.**

Student Name	
Signature	
Date	

APPENDIX 1.3

PERMISSION FORM FOR STUDENTS IN KEY STAGE 5 ONLY

- **Parent / Carer to read and complete**
- **Student to read and complete**

Sixth Form students are permitted to use their own SIM enabled mobile devices during their free time in school, and in selected structured lessons under the supervision of staff. At other times, personal mobile devices brought into school will be stored in a secure location, other than those used specifically for learning during school hours eg AAC device.

If bringing a mobile device into school to be used for educational purposes during school hours eg a mobile phone

The Federation acknowledges that Sixth Form students, whilst working towards 'Preparing for Adulthood', need to learn how to use their own personal devices. The curriculum has been developed to allow selected Sixth Form students to access their own personal mobile device during the school day. Reasonable precautions have been taken to protect the wellbeing of our students and staff while using mobile devices. These precautions are outlined below:

- The mobile device will be accessible to students for certain parts of the day, normally lunchtimes for personal use and specified lessons for educational use;
- The mobile device must only be used in a designated room (eg common room) with a member of staff supervising. Use in teaching areas and when off site to be agreed with the Class Teacher beforehand;
- Staff reserve the right to view and if necessary, confiscate the mobile device until further notice if there is a cause for concern;
- Students will not have access to the school's WiFi network;
- Students will attend online safety sessions and demonstrate an understanding of elements of online safety prior to being given access to their mobile phones;
- Parents & carers will have read and signed an agreement that acknowledges their role in keeping their child and other students safe. As part of this agreement, parents are made aware that the Learn to Live Federation is not responsible for any damage to the mobile device, and that they are responsible for addressing any breach of the parent or student agreements;
- Students will be supported in understanding the rules around acceptable use of their personal mobile device and will need to sign their agreement prior to using their mobile device.

If bringing a mobile device into school to be used for educational purposes during school hours eg an AAC device to support a young person's learning

- Access to the Federation's wireless network entails personal responsibility and compliance with all school rules. Access to the Federation's wireless network will be at the discretion of the school based on the requirements for access.
- Internet access in school must only be via the school's network. Any device with independent access to the internet (mobile phones or other devices with SIM cards) must not be used in school without prior knowledge and permission of the Class Teacher. Unless the device is being used in a specific lesson, devices where the SIM card cannot be removed must not be used during the school day and will held in a secure location and not accessed.
- The school reserves the right at any time to monitor, inspect and if necessary confiscate any mobile device brought into school. Pupils will adhere to teacher and staff instructions regarding the use of mobile devices at all times especially when in class.
- The use of personal mobile devices must not be a disruption or a distraction to teachers or other pupils.

FOR PARENTS & CARERS IN KEY STAGE 5 ONLY:

- **I sign this form and confirm I have read and agree with the Federation's Online Safety Policy.**
- **I agree to allow my young person to use their mobile device for the purposes outlined in Appendix 1.**
- **I understand that every precaution will be taken by staff to ensure that my young person is safe whilst using their own mobile device but that the risks associated with using the internet or mobile devices is ever present.**

Student Name	
Parent / Carer Name	
Signature	
Date	
Make / Model of Device(s)	
Mobile Number (if applicable)	

FOR STUDENTS IN KEY STAGE 5 ONLY:

- **I understand I will take part in online safety lessons and know that I must keep my personal information safe.**
- **I know where I can get online safety help, if I need it.**
- **I understand that I must follow the rules set out below in order to use my own mobile device:**
    - **I will not take photographs or videos of other students or members of staff.**
    - **I must not create, upload or share any inappropriate messages or images, including swearing or comments about others.**
    - **I will not access inappropriate materials when I go online.**
    - **I will only text or call the people on the list approved by my parent /carer.**
    - **I will only access the sites and apps that are on the list approved by my parent /carer.**
    - **My phone/mobile device must be handed in at the start of the day.**
    - **I will only use my device in the specified location, at a time when I am advised.**
    - **I will allow staff to see what I am doing if they ask.**
    - **I will hand my phone/mobile device in at the end of the session and this can be collected at the end of the school day.**
    - **If I am found to be breaking any of these restrictions, I will not be allowed to use my mobile device on site.**

Student Name	
Signature	
Date	

APPENDIX 2

ICT ACCEPTABLE USE AND ICT CODE OF CONDUCT

TO BE READ IN CONJUNCTION WITH THE FEDERATION'S ONLINE SAFETY POLICY

Digital technologies have become integral to the lives of everyone, including children and young people, both within schools and in their lives outside school. The internet and digital technologies are powerful tools, which can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. The Federation 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 Learn to Live Federation's ICT Acceptable Use and ICT Code of Conduct Policy is intended to ensure:

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

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

To view a copy of the Learn to Live Federation's ICT Acceptable Use and ICT Code of Conduct Policy, please contact the Federation ICT Manager.

Users

Learn to Live Federation Staff

Staff are expected to read and sign this Policy prior to being given access to school systems or ICT equipment. A copy will be provided by the Federation ICT Manager at the commencement of employment.

Community Users eg NHS Employees

Community users such as NHS employees will be responsible users and stay safe while using systems and devices. This policy applies to any personal devices that are brought onto a school site.

Users will:

- not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist and extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. Users must not try to use any programmes or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials;
- immediately report any illegal, inappropriate or harmful material or incident they become aware of, to the appropriate person;
- not use personal equipment to record images, without permission. If images are published with consent from the parent or carer, it will not be possible to identify by name, or other personal information, those who are featured;
- not publish or share any information obtained whilst in the school on any personal website, social networking site or through any other means, unless there is prior permission in writing from the school;
- not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work;
- not disable or cause any damage to school equipment, or the equipment belonging to others;
- immediately report any damage or faults involving equipment or software, whatever the cause.

APPENDIX 3

COMPUTER MISUSE AND CYBER CHOICES

TO BE READ IN CONJUNCTION WITH THE FEDERATION'S ONLINE SAFETY POLICY

Purpose

The purpose of this appendix is to set out the Federation's approach to preventing, identifying and responding to computer misuse and potential cybercrime involving learners.

Computer misuse is recognised as a safeguarding issue and this appendix supports the Federation's wider safeguarding, Online Safety, Filtering and Monitoring, Technical Security and Cyber Security arrangements.

This policy aligns with Keeping Children Safe in Education (KCSiE), the Computer Misuse Act 1990, National Crime Agency (NCA) Cyber Choices guidance, and DfE Filtering and Monitoring and Technical Standards.

Scope

This appendix applies to:

- all learners, staff and Governors;
- behaviour occurring within and outside school where it impacts the school community.

Statement

The Federation will ensure that:

- learners understand that some online activity is illegal;
- Bring Your Own Device agreements clearly outline expectations and consequences;
- computer misuse is treated as a safeguarding concern in the first instance;
- staff understand emerging cyber risks and referral routes;
- concerns are referred immediately to the Designated Safeguarding Lead (DSL) and Federation ICT Manager;
- appropriate external advice or referral is sought where required.

Prevention and Education

The Federation will ensure that:

- learners are taught about the Computer Misuse Act 1990 and cybercrime risks;
- curriculum provision promotes ethical and lawful digital behaviour;
- online safety education addresses hacking, malware, phishing, denial-of-service activity and data misuse;
- learners are signposted to positive pathways for developing cyber skills;
- staff are aware of NCA Cyber Choices guidance and resources.

Roles and Responsibilities

- Governors provide strategic oversight of safeguarding and cybercrime prevention;
- Senior Leaders ensure preventative education is delivered and staff are appropriately trained;
- the Designated Safeguarding Lead (DSL) and Federation ICT Manager assesses concerns, completes safeguarding risk assessments, maintains records via CPOMS and seeks external advice where appropriate;
- technical staff monitor network use in line with the Filtering and Monitoring Policy and report concerns to the Federation ICT Manager;
- all staff must report suspected computer misuse immediately and reinforce legal and ethical expectations.

Identification and Reporting

Computer misuse may include:

- unauthorised access to systems or accounts;
- attempting to bypass filtering or monitoring controls;
- use of malware or hacking tools;
- denial-of-service activity;
- password harvesting or credential sharing;
- data theft or system interference.

Where concerns arise, the matter will be referred to the DSL and Federation ICT Manager, a safeguarding risk assessment will be completed, and parents & carers will be informed unless doing so would increase risk.

Referral to Cyber Choices

Where appropriate, the Federation may consult or refer to the local Cyber Choices team via the Regional Organised Crime Unit (ROCU). Cyber Choices is recognised as an early-intervention safeguarding pathway designed to divert young people away from cybercrime.

Support and Risk Management

The Federation will ensure that:

- risk assessments are proportionate and regularly reviewed;
- educational and behavioural support is provided;
- learners are supported to redirect technical skills positively;
- safeguarding responses are consistent with the wider safeguarding framework.

Training and Awareness

The Federation will ensure that:

- staff receive safeguarding updates relating to computer misuse risks;
- DSLs understand referral routes and thresholds;
- Governors understand oversight responsibilities;
- Parents & carers are signposted to relevant guidance where appropriate.

APPENDIX 4

FILTERING AND MONITORING

TO BE READ IN CONJUNCTION WITH THE FEDERATION'S ONLINE SAFETY POLICY

Purpose

The purpose of this appendix 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 appendix applies to:

- all users of the school's ICT 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;
- DSLs and the Federation ICT Manager lead safeguarding responses arising from filtering or monitoring alerts;
- the Federation ICT Manager maintains systems and provides reports as agreed;
- all staff report concerns relating to access, alerts or system effectiveness.

Statement

The Federation 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 Federation 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;
- 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 (eg staff and learners);
- are reviewed regularly to avoid inappropriate over-blocking that may restrict teaching and learning,

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

The Federation will use recognised tools and guidance to assure the effectiveness of filtering provision.

Monitoring

The Federation 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.

Monitoring should be proportionate to the Federation'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 5

TECHNICAL SECURITY

TO BE READ IN CONJUNCTION WITH THE FEDERATION'S ONLINE SAFETY POLICY

Purpose

This appendix sets out how the Federation 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 appendix 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.

Statement

The Federation 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 Federation 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 where appropriate;
- administrator access is restricted and monitored.

System Security and Maintenance

The Federation 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 and regularly tested;
- physical access to infrastructure is controlled.

Device Management

The Federation 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;
- agreements reference responsible device use eg Bring Your Own Device agreement;
- users receive guidance on safe and appropriate device use.

Supplier Management

The Federation 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 6

CYBER SECURITY

TO BE READ IN CONJUNCTION WITH THE FEDERATION'S ONLINE SAFETY POLICY

Purpose

This appendix sets out how the Federation prevents, detects, responds to and recovers from cyber threats. It supports the Federation'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 appendix 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.

Statement

The Federation 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 Federation community.

Cyber Security Strategy

The Federation 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 Federation will ensure that suppliers:

- can demonstrate adherence to and alignment with the DfE Cyber Security Standards.
- are familiar with the Federation's school incident response procedures and able to respond effectively.

Awareness and Education

The Federation 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 Federation 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 Federation will engage external expertise to assess cyber resilience and will work towards recognised standards or certifications. Lessons learned from managing incidents should inform improvements to the strategy.

APPENDIX 7

ELECTRONIC DEVICES: SEARCHING, SCREENING AND CONFISCATION

TO BE READ IN CONJUNCTION WITH THE FEDERATION'S ONLINE SAFETY POLICY

Purpose

The purpose of this appendix is to set out the Federation's lawful and proportionate approach to searching, screening and confiscating electronic devices and examining or deleting data from those devices.

This appendix supports the Federation's safeguarding responsibilities and must be read alongside the Behaviour Policy and the Safeguarding & Child Protection Policy.

This appendix reflects Keeping Children Safe in Education KCSiE), DfE Searching, Screening and Confiscation guidance, DfE Behaviour in Schools guidance and relevant statutory legislation.

Scope

This appendix applies to:

- all learners;
- all authorised staff;
- all electronic devices in a learner's possession;
- devices on school premises or used in connection with school activities;
- behaviour occurring both on and off site where it impacts safeguarding or discipline.

Statement

The Federation will ensure that:

- searches are lawful, proportionate and necessary;
- safeguarding considerations are prioritised;
- devices are only searched where there are reasonable grounds;
- deletion of data is undertaken only where there is a lawful and justifiable reason;
- criminal matters are referred to LADO/the Police;
- incidents are recorded securely;
- staff are appropriately trained.

Authorised Staff

- the Executive Head will authorise in writing those staff permitted to conduct searches, examine devices and delete data;
- authorised staff will receive appropriate training including safeguarding, legal thresholds and digital evidence handling;
- staff cannot be required to undertake searches.

Screening

Where screening measures are used, they will:

- be clearly communicated to learners and parents;
- be proportionate and risk-based;
- be implemented consistently;
- support a calm, safe and orderly environment.

Searching for Electronic Devices

Electronic devices may be searched with consent or without consent where permitted by legislation. Force will not be used to search for items banned under school rules.

Searches will:

- be conducted by authorised staff;
- be carried out privately where possible;
- involve removal of outer clothing only;
- not extend to intimate searches.

Examination of Electronic Devices

- staff may examine data where there is a good reason to do so, including where data poses a safeguarding risk;
- examination will extend only as far as reasonably necessary to establish the facts;
- where indecent images of a child are suspected, staff must not intentionally view the image and must refer immediately to the DSL;
- where material may constitute a criminal offence, the device will be handed to the Police.

Deletion of Data

- data may only be deleted where there is a safeguarding reason and the material is not required as evidence;
- deletion decisions must be proportionate and recorded;
- material that may constitute criminal evidence must not be deleted.

Safeguarding Response

All incidents involving device searches will:

- be referred to the DSL;
- be recorded via CPOMS under “safeguarding”;
- trigger a risk assessment where appropriate;
- involve parents & carers unless doing so would increase risk.

Care of Confiscated Devices

The Federation will ensure secure storage of confiscated devices, documentation of chain of custody and appropriate return procedures.

Training

The Federation will ensure that:

- authorised staff receive specialist training;
- DSLs understand legal thresholds;
- all staff are aware of reporting expectations;
- Governors understand oversight responsibilities.

Monitoring and Review

The Federation, via CPOMS, will maintain records of searches and data deletion.

APPENDIX 8

PUBLIC ONLINE COMMUNICATIONS

TO BE READ IN CONJUNCTION WITH THE FEDERATION'S ONLINE SAFETY POLICY

Purpose

The purpose of this appendix is to set out how the Federation 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 appendix supports the Federation's Online Safety Policy 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 appendix 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.

Statement

The Federation will ensure that:

- public online communications are accurate, lawful and appropriate;
- safeguarding considerations are prioritised;
- personal data is protected;
- 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 appendix, 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 Federation 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 Federation will ensure that:

- appropriate consent is obtained;
- images are appropriate and dignified;
- learners are not identified unnecessarily eg student forename/full name;
- images are removed where consent is withdrawn;
- to reduce the risk of illegal manipulation of publicly available images of staff and learners, the Federation is aware of how images can be shared online (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:

- personal use must not impact professional standards nor school reputation;
- staff must not engage with students via personal accounts.

Handling Complaints and Abuse

Where negative comments are made online:

- the school will respond proportionately;
- abusive content should be challenged and removed, where possible eg reported to Facebook;
- 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 Federation will ensure that:

- staff responsible for public accounts receive guidance and training;
- Governors understand oversight responsibilities;
- the wider community is informed of expected standards.

LINKS TO ORGANISATIONS AND DOCUMENTS

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

CEOP
CEOP - http://ceop.police.uk/
ThinkUKnow - https://www.thinkuknow.co.uk/

Others
Kent – Online Safety Resources page
INSAFE/Better Internet for Kids - https://www.betterinternetforkids.eu/
UK Council for Internet Safety (UKCIS) - https://www.gov.uk/government/organisations/uk-council-for-internet-safety
Tools / Resources for Schools / other organisations
Whisper Anonymous Reporting Tool - https://swgfl.org.uk/products/whisper/
360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/
SWGfL Test filtering - http://testfiltering.com/
SWGfL 360 Groups – online safety self review tool for organisations working with children
SWGfL 360 Early Years - online safety self review tool for early years organisations
Childline – Report / Remove
SWGfL- Assisted Monitoring
SWGfL – Resources for Education
DfE Using AI in education settings: support materials

Bullying/Online-bullying/Sexting/Sexual Harassment
Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - http://enable.eun.org/
Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
Childnet – Cyberbullying guidance and practical PSHE toolkit:
http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit
Childnet – Project deSHAME – Online Sexual Harrassment
UKSIC – Sexting Resources
Ditch the Label – Online Bullying Charity
Diana Award – Anti-Bullying Campaign

Social Networking
UKSIC - Safety Features on Social Networks

Children's Commissioner, TES and Schillings – Young peoples' rights on social media

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

Data Protection
DfE – Data Protection in schools toolkit
ICO Guides for Organisations
ICO Guidance on taking photos in schools

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

Infrastructure/Technical Support/Cyber Security
DfE – Technical Standards for Schools and Colleges
UKSIC – Appropriate Filtering and Monitoring
SWGfL Safety & Security Resources
SWGfL - Cyber Security in Schools
NCA – Guide to the Computer Misuse Act
SWGfL- Assisted Monitoring
Secure Schools – Cyber Security

Working with Parents & Carers
Childnet Webpages for Parents & Carers
Get Safe Online - resources for parents
Teach Today - resources for parents workshops/education
Internet Matters

Prevent
Prevent Duty Guidance
Childnet – Trust Me

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

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