NEWCASTLE SCHOOL FOR BOYS

ICT & ONLINE SAFETY POLICY

May 2026

CONTENTS

Appendices

SECTION 1 - INTRODUCTION

1. Introduction, Purpose & Scope

1.1 **Purpose**

This policy sets out how Newcastle School for Boys (the School) ensures the safe, responsible, lawful and ethical use of digital technologies. It integrates online safety, ICT acceptable use, cyber security, 1:1 device use, digital safeguarding expectations, and generative AI governance into a single document.

This policy should be read alongside the School's Safeguarding & Child Protection Policy and Behaviour Policy.

1.2 **Purpose**

The purpose of this policy is to:

- Protect pupils, staff and the wider school community from online harms, including content, contact, conduct and commerce risks identified in statutory guidance.
- Ensure compliance with the Independent School Standards and statutory safeguarding duties.
- Embed online safety as a whole school safeguarding responsibility in line with KCSIE 2025.
- Provide a structured, future ready framework for safe and effective digital learning, including AI use.
- Establish clear expectations for all users of school technology, including staff, pupils, contractors, visitors and parents.

1.3 **Scope**

This policy applies to:

- All staff (teaching, support, contractors, visiting professionals)
- All pupils from EYFS upwards
- Parents and carers
- Governors and trustees
- Visitors and volunteers
- All school owned devices, networks, platforms and systems
- All personal devices used on the school site or connected to school services (BYOD)
- All remote/online learning environments and digital communications

This policy covers all use of technology *on school premises* and *off-site* when accessing school platforms or engaging in school activities.

2. Legal and Regulatory Framework

This policy is written in accordance with the statutory and regulatory frameworks that govern safeguarding, online safety, digital systems, and educational provision.

These include:

- **Independent School Standards (DfE/ISI)**, which require robust leadership and management of safeguarding, welfare, and information provision.
- **Keeping Children Safe in Education (KCSIE) 2025**, which states that online safety is an essential part of whole school safeguarding and must be embedded across all practice. It requires schools to educate pupils, train staff, implement filtering and monitoring, and manage cybersecurity risks.
- **DfE Digital & Technology Standards (2026)**, which outline expectations for digital leadership, cyber security, filtering and monitoring systems, infrastructure, and IT governance.
- **DfE Filtering & Monitoring Core Standard (2026)**, requiring schools to ensure their filtering and monitoring systems protect users from illegal and harmful content, without unreasonably restricting teaching and learning. Schools must review their filtering and monitoring at least annually and clearly allocate responsibilities for oversight.
- **DfE Generative AI in Education Policy (2025)**, which explains that AI must be used safely, legally, ethically, and transparently; that data protection and safeguarding risks must be assessed; and that schools must ensure pupils are not disadvantaged or exposed to harm through AI use.
- **UKCIS Guidance on 'Sharing Nudes and Semi Nudes' (2024 update)**, which provides statutory aligned procedures for responding to youth produced sexual imagery incidents and instructs that staff must not view, copy or share illegal imagery.
- The **Data Protection Act 2018** and **UK GDPR**, regarding safe handling of personal data.
- The **Education Act 2011** and **Computer Misuse Act 1990**, which help regulate access to information and digital systems.

This policy helps the school meet the independent School Standards by ensuring strong digital safeguarding, clear staff responsibilities, and secure online practices. It supports requirements relating to pupil welfare, staff reviewing the suitability of online material, leadership and management, and the safe operation of ICT systems, demonstrating that the school maintains a safe, well-governed digital environment.

3. Roles and Responsibilities

3.1 Governing Body

- Ensures that safeguarding, online safety and digital standards meet statutory requirements.
- Receives annual reports on filtering and monitoring effectiveness and assures itself that systems are appropriate, effective and meet DfE standards.
- Approves this policy and monitors its implementation.

3.2 Chief Operating Officer

- Ensures whole school compliance with this policy.
- Allocates staffing, resources and time for staff training, filtering/monitoring, and digital safeguarding oversight.

3.3 **Designated Safeguarding Lead (DSL)**

- Leads on online safety, including filtering and monitoring oversight; manages incidents, referrals and risk assessments.
- Ensures staff are trained and supported.
- Liaises with external agencies as required.
- Keeps up to date with online safety guidance from CEOP, Childnet, UKCIS, the local safeguarding partnership and other recognised bodies.

3.4 **IT Network Manager**

- Implements and maintains secure IT systems; manages filtering/monitoring tools; ensures patching, backups and network security meet DfE standards.
- Supports the DSL by providing alerts, logs and technical evidence for safeguarding.

3.5 **All Staff**

- Model safe, respectful use of technology.
- Follow the Staff Acceptable Use Agreement and any device agreements.
- Report online concerns immediately to the DSL.
- Use AI only in approved, safe, ethical ways.
- Follow data protection and cyber security guidance.

3.6 **Pupils**

- Follow the Pupil Acceptable Use Agreement and any device agreements.
- Report anything worrying or inappropriate.
- Use digital tools responsibly, safely and legally.
- Use AI only when explicitly allowed and always honestly.

3.7 **Parents/Carers**

- Support safe online behaviour at home.
- Engage with school provided guidance on digital resilience.
- Report concerns promptly.

SECTION 2 – ONLINE SAFETY

4. Online Safety Education & Digital Literacy

Online safety education at the School addresses the four areas of online risk defined in 2025 (content, contact, conduct and commerce). Pupils are taught how to recognise, avoid and report risks across all four categories, including harmful or age inappropriate content, unsafe online contact, risky or illegal online behaviours, and commercial or financial harms such as scams or misleading advertising.

4.1 **Whole School Approach**

Online safety is embedded throughout the curriculum and the wider school culture. KCSIE 2025 states that schools must take a whole school, embedded approach to online safety, ensuring that pupils are taught about safeguarding, including online harms, across subjects and through planned curriculum opportunities.

Digital literacy, digital citizenship and responsible behaviour are taught at an age appropriate level from Year 1 upward.

Staff must ensure pupils are appropriately supervised when using school devices or accessing the internet.

4.2 **Curriculum Coverage**

As an all-boys school, our online-safety education and monitoring recognise increased exposure among boys to misogynistic content and influencers, certain high-risk online challenges, gambling-like mechanics and financial scams, and targeted radicalisation narratives. Our RSHE/PSHE, tutor time and assemblies explicitly address respectful relationships, sexual harassment/violence online, and critical evaluation of online personas and "parasocial" relationships.

Online safety is delivered through:

- Computing curriculum (safe use of networks, critical evaluation of online content, digital footprints)
- PSHE/RSHE (healthy online relationships, consent, harmful content, grooming, online sexual harassment)
- Subject specific contexts (research skills, copyright, academic honesty)

Curriculum content addresses the DfE defined four categories of risk (content, contact, conduct, commerce), including emerging risks such as misinformation, disinformation and conspiracy theory exposure.

4.3 **Pupils' Critical Thinking & Media Literacy**

Pupils learn to:

- Identify and critique misinformation and disinformation.
- Recognise persuasive design and manipulative online behaviour.
- Understand online bias, echo chambers and algorithmic influence.

4.4 **Vulnerable Pupils**

Teaching is adapted for vulnerable children, including those with SEND, EAL or prior safeguarding concerns, following KCSIE's principle that *"one size does not fit all"*.

4.5 **Parent/Carer Engagement**
The school provides guidance, workshops and updates to parents/carers on digital risks and household digital safety.

5. Cyber Bullying

Cyberbullying includes harassment, threats, humiliation, impersonation, and sexualised behaviours using digital technologies.

Parents and carers are expected to take primary responsibility for monitoring their child's online activity, promoting appropriate behaviour, and addressing any misuse of digital platforms outside of school hours.

The School will respond to incidents of cyberbullying where they are reported and have a demonstrable impact on pupil welfare or the school community, including cases that occur outside of school.

6. Filtering & Monitoring

6.1 **Statutory Requirements**
In line with the DfE Filtering & Monitoring Core Standard and KCSIE 2025, the school must maintain a safe online environment through effective filtering and monitoring. These systems form a core part of our safeguarding arrangements and must prevent access to harmful or inappropriate content while supporting legitimate teaching and learning.

6.2 **Key Features of Filtering**
Our filtering system:

- Blocks illegal content, including extremist or terrorist material.
- Blocks harmful or inappropriate categories such as adult content, self-harm, violence, and drugs.
- Avoids *over-blocking* to ensure staff can access legitimate resources needed for teaching, as advised by the DfE.

6.3 **Key Features of Monitoring**
Our monitoring system:

- Alerts the ICT Team and DSL to harmful keywords, unsafe behaviours, or concerning content.
- Includes classroom supervision tools and device management functions.
- Generates regular reports reviewed by the DSL and ICT Network Manager.

The ICT Network Manager ensures our filtering methods remain appropriate, effective, and proportionate. Periodic checks are carried out using the SWGfL test site. Any material believed to be illegal is reported to the police.

All staff share responsibility for reporting inappropriate material. Concerns must be passed to the ICT Network Manager, ICT Technician, or DSL.

Our firewall and filtering systems are designed to prevent staff and pupils from accessing or downloading offensive, abusive, or sexually explicit material.

Occasional accidental access may occur due to the changing nature of online content and methods used to bypass filters. Anyone who unintentionally accesses such material must report it immediately to the ICT Network Manager / ICT Technician / DSL. Staff and pupils will not be held responsible when reporting accidental access promptly.

6.4 **Roles & Responsibilities**

DfE standards require clear assignment of responsibilities:

- **SLT:** Strategic oversight, procurement of filtering/monitoring solutions, and review of system effectiveness.
- **DSL:** Interprets cpoms monitoring data, escalates concerns, and leads the safeguarding response.
- **ICT Network Manager:** Technical management, maintenance, testing, and provision of evidence for review.

6.5 **Annual Review**

Filtering and monitoring arrangements are reviewed as part of the annual safeguarding audit led by the DSL, link governor for safeguarding and the school's safeguarding consultants.

6.6 **Self-Assessment**

The school uses the DfE *Plan Technology for Your School* self-assessment tool to evaluate compliance and identify areas for improvement.

7. Cyber Security & Data Protection

7.1 **Cyber Security**

The school meets the DfE's Cyber Security Standard, which requires secure user accounts, MFA where available, regular patching and updates, and secure backups. Key features include:

- Firewalls, anti-malware protection.
- Strong password enforcement.
- Secure configuration and access control.
- Staff cyber awareness training (annual minimum).

7.2 **Data Protection**

All processing of personal data complies with UK GDPR and the Data Protection Act 2018.

Staff must:

- Only store data on approved, encrypted platforms.
- Never transfer personal data to unauthorised devices.
- Follow the school's Data Protection Policy.

All digital processing follows the principles of data minimisation and lawful purpose under UK GDPR.

7.3 **Remote Access**
Remote access is via secure VPN or approved cloud platforms, in line with DfE guidance on secure remote access.

7.4 **Supply Chain Assurance**
Suppliers are vetted, considering security posture and certifications where applicable.

8. Incident Management, Searching & Escalation

8.1 **Reporting Concerns**
Online safety is an integral part of our whole school safeguarding arrangements and must be considered alongside the Child Protection and Safeguarding Policy. All concerns must be reported immediately to the DSL or Deputy DSL.

8.2 **Youth-Produced Imagery ("Nudes/Semi-Nudes")**
The school follows UKCIS (2024) guidance. Staff must:

- Not view, copy, save, store, or share any imagery.
- Refer the incident to the DSL, who will complete a formal risk assessment.
- Involve the Police where required by law or where the risk assessment identifies significant harm.

8.3 **Illegal Content**
All illegal content is immediately escalated to the DSL and, when required, the Police.

8.4 **Searching & Confiscation**
Searching and confiscation follow the DfE guidance "Searching, Screening and Confiscation", as referenced in KCSIE 2025. Devices may be secured for safeguarding or evidential purposes.

Under the Education Act 2011, the Headteacher and authorised staff may search pupils and confiscate devices when they have reasonable grounds to suspect that an item:

- Poses a risk to staff or pupils, and/or
- Is listed as a banned item in school rules, and/or
- May provide evidence relating to an offence.

Examples include:

- Pornographic material
- Abusive messages, images or videos
- Indecent images of children
- Material relating to suspected criminal behaviour (e.g., threats or violence)

Before a search authorised staff must:

- Assess urgency and risk to pupils and staff. If not urgent, seek advice from the Headteacher or DSL.
- Explain to the pupil why the search is required, how it will be conducted, and answer any questions.
- Seek cooperation. If the pupil refuses, staff will follow the school Behaviour Policy.

Authorised staff must:

- Inform the DSL of any search where banned items were reasonably suspected.
- Involve the DSL immediately if the search reveals a safeguarding concern.

Staff may examine, and in exceptional circumstances, erase data on a confiscated device where there is a good reason, meaning a reasonable belief that the data may be used to:

- Cause harm, and/or
- Undermine school safety or disrupt teaching, and/or
- Commit an offence.

If inappropriate material is found, staff (with the DSL/Headteacher) will decide on the appropriate response, prioritising safeguarding.

Where material may be evidence of a criminal offence, no deletion will occur; the device will be passed to the Police as soon as practicable.
Material may be deleted only when:

- Its continued existence is likely to cause harm, and/or
- The pupil or parent refuses to delete it themselves, and
- It is not suspected to be evidence of an offence.

If staff suspect a device contains indecent images of a child, they must:

- Not view the image.
- Not copy, print, store, or share the image.
- Confiscate the device and report immediately to the DSL.

The DSL will act in accordance with:

- DfE *Searching, Screening and Confiscation* guidance
- UKCIS *Sharing Nudes & Semi-Nudes* guidance

All searches of pupils must follow:

- The DfE's latest Searching, Screening and Confiscation guidance
- UKCIS guidance on Sharing Nudes & Semi-Nudes
- Relevant sections of KCSIE

Complaints relating to searches or deletion of files will be managed through the school's Complaints Procedure.

9. Training & Awareness

- **Staff:** mandatory induction + annual safeguarding/online safety updates.
- **DSL:** enhanced training; must stay current with online risks and digital standards.
- **Governors:** training in digital safeguarding, AI governance and filtering/monitoring oversight.
- **Pupils:** recurring digital literacy and online safety education.
- **Parents:** access to guidance, workshops and online safety communications.

SECTION 3 - ICT & ACCEPTABLE USE

10. Unacceptable use

The following behaviour is considered unacceptable use of the school's ICT facilities. Breaches of this policy may result in disciplinary action in accordance with the school's Behaviour Policy (for pupils) or Disciplinary Procedures (for staff).

Unacceptable use includes, but is not limited to:

- Breaching copyright or intellectual property rights.
- Using ICT facilities to bully, harass, intimidate or unlawfully discriminate against others.
- Violating any school policy or procedure.
- Any illegal conduct or statements that promote or encourage unlawful activity.
- Online gambling, inappropriate advertising, phishing, fraud, or other financial scams.
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene, harmful or otherwise inappropriate.
- Consensual or non-consensual sharing of nude or semi-nude images, videos, or livestreams.
- Activity that defames, damages, or risks bringing the school into disrepute.
- Sharing confidential or sensitive information about the school, pupils or staff without authorisation.
- Connecting personal devices to the school network without approval.
- Installing or running unauthorised software, applications, or web services on the school network.
- Creating or using any programme or tool designed to interfere with the school's ICT systems, accounts or data.
- Accessing, or attempting to access, restricted or password protected areas without approval.
- Enabling, assisting or encouraging others to access ICT systems without permission.
- Causing intentional damage to ICT equipment or systems.
- Removing, deleting or disposing of the school's ICT equipment, data or systems without permission.
- Causing a data breach by accessing, modifying or sharing information (including personal data) without authorisation.
- Using offensive, discriminatory or inappropriate language online.
- Promoting a private business unless directly authorised by the school.
- Using tools or websites to bypass the school's filtering or monitoring systems.
- Engaging in extremist, radicalised, homophobic, racist, antisemitic or otherwise discriminatory content or conduct.
- Using AI tools or generative chatbots (e.g., ChatGPT, Google Gemini) for:
    - Internal or external assessments, or coursework.
    - Classwork or homework where AI generated content is presented as the pupil's own work.

This list is not exhaustive. The school may determine that other behaviours constitute unacceptable use. The Headteacher and relevant staff will use professional judgement when assessing behaviour not explicitly listed above.

10.1 **Exceptions from unacceptable use**

Where the use of ICT facilities is required for a legitimate purpose that would otherwise fall under "unacceptable use," an exemption may be granted at the Headteacher's discretion. Requests must be made in writing before the activity takes place.

10.2 **Sanctions**

Pupils or staff who engage in unacceptable use may face sanctions in accordance with:

- The school's Behaviour Policy (pupils)
- The Staff Disciplinary Procedures (employees)
- Any relevant safeguarding procedures

11. STAFF

11.1 **Access to School ICT Facilities & Materials**

The school's IT Network Manager, manages access to the school's ICT facilities and materials for staff. That includes, but is not limited to:

- Computers (desktop and laptops) tablets, mobile phones and other devices.
- Access permissions for certain programmes or files.

Staff are provided with unique login/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the ICT Network Manager.

11.2 **Staff 1:1 Devices (laptops / iPads)**

Staff may be issued with a school laptop / iPad to support teaching, administration and wider professional duties. All devices remain the property of the School and must be used in line with the Staff Acceptable Use Agreement, Data Protection Policy, and all relevant safeguarding expectations. Staff are expected to engage with training and guidance provided for effective and safe use of their school device.

School laptops / ipads are provided for professional use, including teaching, planning, administration, communication and training. Limited personal use is permitted, provided it complies with the conditions set out in this policy, does not interfere with work, and does not breach safeguarding, cyber-security or data protection requirements.

Staff must:

- Use the device primarily for work-related tasks.
- Ensure all school business is conducted only via approved platforms (e.g. school email, Office 365, secure cloud services).
- Avoid storing personal files on the device or school network.
- Ensure pupils never use or access a staff laptop.

- Follow school guidance on the safe use of email, internet access, data handling and AI tools.
- Lock or log off devices whenever they are left unattended to prevent unauthorised access.

Staff must not install unauthorised applications, disable security features, or attempt to alter device management settings.

All school devices are centrally configured. Staff must not install, remove or modify apps or system settings except through approved IT processes.

Staff are responsible for taking reasonable care of their laptop, including:
- Keeping the device in a protective case when transporting it.
- Avoiding damage from drops, pressure, liquids or extreme temperatures.
- Ensuring the device is charged and ready for professional use.
- Promptly reporting faults through the school's IT support system.

Loss or damage resulting from neglect or misuse may incur costs not covered by the School's insurance.

School laptops are managed and monitored by the IT Network Manager in line with DfE Digital & Technology Standards. Staff must:
- Keep the device secure and never leave it unattended in unsecured locations.
- Use strong passwords and comply with MFA and password-reset requirements.
- Store all school data only on approved, encrypted platforms.
- Never allow family members or others to use the device.
- Report loss, theft or suspected compromise immediately to IT Support and the COO/DSL as appropriate.

Where a device is lost or stolen outside school, staff must report the incident to the police as required and provide the School with relevant information (e.g. crime reference number).

Staff laptops are subject to filtering, monitoring and technical oversight for safeguarding, cybersecurity and operational purposes. The School may audit, secure, lock or remotely wipe devices if needed to protect users or data. There is no expectation of privacy when using school devices or systems.

When a staff member leaves the School or no longer requires the device, it must be returned, with charger and accessories, on or before their final working day.

11.3 **Personal Devices**

Personal devices include any non-school-issued phones, tablets, laptops, smartwatches, storage media or wearable technology.

11.3.1 **Principles**

- School business should be conducted on **school-issued devices** wherever possible.

- Staff may bring personal devices onsite, but use must remain **safe, lawful, professional** and aligned with safeguarding duties.
- Pupils must **never** access or use a member of staff's personal device.
- Devices must be silenced and **not used during lessons, duties or supervision** except in emergencies.
- No personal device use in the presence of pupils unless operationally necessary.

11.3.2 **Safeguarding, Privacy & Monitoring**

- Personal device use must always support safeguarding and confidentiality.
- If a personal device used for school access is lost, stolen or compromised, staff must report it immediately to IT and the DSL if relevant.
- Any device accessing school systems may be subject to monitoring; there is no expectation of privacy for school-related activity on personal devices.

11.4 **Use of Emails**

Email is an essential tool for supporting the school's internal and external communication. As with all written communication, staff must take particular care when composing messages, as tone and intent can be easily misinterpreted, and all email content may be subject to scrutiny. Effective email use contributes directly to safeguarding, data protection and professional conduct expectations outlined in statutory guidance such as *Keeping Children Safe in Education (KCSIE)*, which requires staff to communicate professionally and maintain appropriate boundaries with pupils and families.

All staff are issued with a school-approved email account, and all school-related communication must be conducted using this account only. Personal email accounts must never be used for school business. Staff must enable multi-factor authentication (MFA) where available. Staff must not share their personal email addresses with pupils or parents/carers, and must not send any work-related information from personal addresses.

Staff must take particular care when composing messages. Improper statements may create risks including defamation, harassment, discrimination, breach of confidentiality, or breach of contract.

Emails may be disclosed in legal proceedings or through requests under data-protection legislation. Staff should assume that all email content is potentially retrievable, even after deletion, and ensure their communication is professional, factual and respectful at all times.

When sending sensitive or confidential information, staff must ensure that attachments are encrypted or otherwise appropriately protected to safeguard personal data. If a staff member receives an email in error, they must notify the sender and delete the message. If the email contains personal or confidential information, the staff member must not use or disclose it under any circumstances. If a staff member sends an email containing someone else's personal data in error, they must report the incident to the Chief Operating

Officer immediately and follow the school's data-breach procedure, as required under UK GDPR obligations.

All electronic communication, including email, must be transparent, professional and open to scrutiny. Chain letters, suspicious links, spam, phishing attempts, and emails from unknown or untrusted sources must be deleted without opening.

Staff must not use personal messaging apps, social media accounts or personal email to communicate with pupils or parents under any circumstances.

11.4.1 **Spam and threat filtering**

The school operates an anti-spam and threat-monitoring system, designed to prevent the delivery of junk mail and offensive or harmful content. However, cyber-threats evolve rapidly, and it is possible that inappropriate or explicit material may occasionally bypass filtering. If this occurs, staff must inform the ICT Network Manager or ICT Technician immediately. Staff will not be held responsible for any inappropriate content received in this manner provided they report it without delay.

Upon notification, the ICT Network Manager will inform the Chief Operating Officer, who will assess the situation and escalate to relevant authorities if necessary, in line with safeguarding and cyber-security expectations under DfE Digital Standards.

11.4.2 **Email protection**

Staff must comply with copyright requirements for any material sent or received by email. Staff must not send messages that could unintentionally create a legally binding contract unless they have explicit authorisation to do so.

To reduce risk, the school discourages the unnecessary use of global emails, and may technically restrict bulk messaging or block emails from specified external domains where this supports cyber-security or safeguarding requirements.

All staff must remain aware that emails may be used as evidence in disciplinary procedures, grievances, safeguarding enquiries, Freedom of Information requests, and legal proceedings. This aligns with the principle in KCSIE that all forms of communication may be reviewed where safeguarding concerns arise.

11.5 **Mobile Phones**

Staff must not give their personal phone number(s) to parents/carers or pupils. Staff must use phones provided by the school to conduct all contact with parents / carers, or must withhold their number if calling from a personal device.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use.

11.6 **Acceptable use of the internet**

Staff must use the internet in a way that supports the school's safeguarding responsibilities, maintains professional standards, and complies with all relevant legislation and school policies. Internet access is provided primarily for educational, administrative and operational purposes, and staff are expected to use online resources in a professional, lawful and responsible manner at all times.

Acceptable use includes:

- Accessing online teaching, learning and administrative platforms necessary for fulfilling professional duties.
- Researching educational materials, professional development resources and curriculum-related content.
- Using approved communication systems (e.g., school email) to interact with colleagues, pupils and parents/carers in a professional manner.
- Using school-approved cloud services and systems for the storage and transfer of work-related information, in accordance with data-protection requirements.

Unacceptable use includes, but is not limited to:

- Accessing or attempting to access material that is illegal, harmful, inappropriate, discriminatory or otherwise in breach of school safeguarding expectations.
- Downloading or installing unauthorised software or browser extensions.
- Attempting to bypass, disable or interfere with the school's filtering or monitoring systems.
- Using school internet services to engage in personal commercial activities, gambling, political campaigning or other non-school-related ventures.
- Any activity that may compromise the security of school systems or put pupils, staff or data at risk.

Staff must remain mindful that all internet activity conducted via school devices or networks may be monitored in accordance with the DfE's Filtering and Monitoring Standards. Staff must therefore use the internet in a way that upholds the highest standards of professionalism, maintains a safe learning environment and protects the reputation of the school.

Staff must check online content, search terms, images and websites for suitability before using them with pupils.

11.7 **Personal Use of ICT and the Internet**

Staff may make limited personal use of the internet when using school ICT facilities, provided that such use is appropriate, lawful, and does not interfere with professional responsibilities or the safe operation of the school's network. Personal use should generally take place outside contact time, ideally before or after the school day or during breaks, in order to reduce unnecessary traffic on the school network at peak operational times.

Personal browsing may be subject to monitoring, in line with the school's safeguarding and cyber-security responsibilities. Although the school does not

actively monitor every website accessed by staff, users must understand that there can be no expectation of privacy when using school systems, as technical logs and filtering systems operate continuously to protect pupils and staff.

Staff may use the school's internet for personal purposes only if the following conditions are met:

- Personal use does not take place during lessons, supervision duties, meetings, or any period of direct responsibility for pupils.
- There is no risk of pupils viewing or being exposed to personal content, and personal use does not occur when pupils are present.
- Use does not breach any school policy or constitute unacceptable use, including accessing or attempting to access inappropriate, harmful, or illegal content.
- Use does not prevent others from using ICT resources for teaching, learning or operational purposes.

Personal use must never involve gambling, political campaigning, financial activities, or any purpose that could compromise the security or reputation of the School.

Staff must not save or store personal, non-work-related files (such as photos, music, videos, or personal documents) on school devices or on the school network. Such storage creates unnecessary data management risks and may breach data-security expectations.

Staff should be aware that any personal use of ICT on school systems may fall within the scope of the school's monitoring systems and safeguarding audits. Breaches of this policy, or behaviour indicating misuse of the school's digital infrastructure, may result in disciplinary action in line with school procedures and KCSIE 2025 safeguarding principles.

Staff may use personal devices (such as mobile phones or tablets) on the school site in accordance with the Staff Code of Conduct and relevant safeguarding expectations. Staff should also note that personal online activity conducted off-site, even when not using school ICT, can still affect their professional reputation and employment if it results in personal information becoming public or accessible to pupils or parents/carers.

Staff must take care to follow the school's guidelines on social media use and email conduct in order to protect their professional integrity and to support a safe digital environment for pupils and colleagues.

12. PUPILS

12.1 Access to School ICT Facilities & Materials

Pupils are provided with access to the School's ICT facilities to support learning, research and communication. Access is a privilege and must be used responsibly, safely and in accordance with the Pupil Acceptable Use Agreement and all relevant school policies.

The School's ICT facilities include (but are not limited to) computers, laptops, tablets, 1:1 devices, printers, school-managed accounts, approved software, cloud platforms, and internet services. All pupils are issued with a unique login and password, which must be kept secure.

Pupils must:

- Use only their own login details and never share passwords with others.
- Access ICT facilities only for school-approved learning activities.
- Store work in the School's approved cloud platform (Office 365 OneDrive).
- Report any technical issues, inappropriate content, or security concerns to a member of staff immediately.
- Follow staff instructions regarding safe and appropriate use of ICT equipment.
- Use ICT facilities in line with safeguarding expectations, including the avoidance of harmful, inappropriate, or illegal content.

Pupils must not attempt to access restricted areas, alter device settings, install software, or use any method to bypass the School's filtering or monitoring systems.

The ICT Network Manager controls pupil access to ICT facilities and resources. Access rights may differ depending on a pupil's year group, subject needs or safeguarding considerations. Where access permissions need to be updated, or where a pupil cannot log in, support is available through the School's IT Support Team.

12.2 **Pupil 1:1 Devices**

Pupils in the Senior School are issued with a 1:1 laptop for educational use. The device remains the property of the School and must be used in line with the Pupil Acceptable Use Agreement and all relevant school policies. A "Responsible Use Agreement" must be signed by parents/carers and pupils before a device is issued. When a pupil leaves the School, the device and all accessories (charger, cable, case) must be returned by the final day of attendance.

Device use:

- Devices are for educational purposes only, both in school and at home.
- Use in school is only with a teacher's permission.
- Pupils must follow instructions given by staff and stop using the device when asked.
- Work must be saved to the School's approved cloud platform (Office 365 OneDrive).
- Pupils must not install or remove software, alter system settings, or attempt to access or interfere with another person's device.
- The device must not be used outdoors, on public transport, or in public spaces.

Care of the device:

- Devices must always be carried in the school issued protective case.
- Chargers should be kept at home and devices brought to school fully charged each day.
- Devices must be kept in lockers when not in use and handled carefully to avoid drops, pressure, liquids or extreme temperatures.
- Pupils must report any faults or issues to the IT Support Team as soon as possible via the school's reporting systems.

Loss, damage and insurance:

- Devices are insured under the School's policy; however, wilful damage, neglect or misuse may incur repair or replacement costs for parents/carers where these are not covered by insurance.
- If a device is lost or stolen, this must be reported to the police within 48 hours and to the School as soon as possible, including the crime reference number.

Security and monitoring

- Devices are monitored and managed by the School, including remote locking/wiping when necessary.
- The School uses classroom.cloud to supervise device use and ensure safe and appropriate behaviour.
- Pupils must not attempt to disable monitoring tools, change restrictions, or remove security settings.
- Strong passwords must be used and kept secure; the School can reset passwords where required.

12.3 **Acceptable Use of the Internet**

Pupils may access the internet using school devices or the school network to support learning, research and communication. Internet use must always be safe, responsible and in line with the Pupil Acceptable Use Agreement and all relevant school policies.

The School provides filtered and monitored internet access to help protect pupils from harmful or inappropriate content. However, pupils also have a responsibility to use the internet in a way that upholds the School's safeguarding expectation.

Pupils must:

- Use the internet only for school approved learning activities.
- Access websites, platforms and resources as directed by staff.
- Use their school email account for schoolwork and communication with teachers.
- Save work to the School's approved cloud platform (Office 365 OneDrive).
- Tell a member of staff immediately if they accidentally access anything worrying, inappropriate or harmful.
- Follow instructions given by staff about when and how to use the internet.

Pupils must not:

- Use any method to bypass the School's filtering or monitoring systems.
- Attempt to access restricted areas, private accounts or password-protected content.
- Engage in any behaviour online that is unsafe, inappropriate or harmful.
- Use personal messaging apps, social media or personal email for school purposes.
- Upload, download or share files that are not related to schoolwork.

(Activities that are illegal, unsafe or inappropriate are addressed separately in Section 10 – Unacceptable Use.)

Pupils may only use the internet when a member of staff has given permission, and they must follow all classroom rules and any website restrictions set by teachers. Staff may instruct pupils at any time to close a website, stop using the internet, or hand over their device, and pupils are expected to comply immediately.

Pupils must immediately tell a member of staff or parent/carer if:

- they see or receive something online that makes them feel unsafe, uncomfortable or upset
- they know that another pupil has accessed harmful or inappropriate content
- someone online tries to contact them in an unsafe way

Concerns will be responded to in line with the School's safeguarding procedures.

13. Passwords & Encryption

13.1 Passwords

- Strong passwords**:** All users must set strong, unique passwords for their school accounts and keep them confidential.
- Account responsibility**:** Users are responsible for the security of their accounts and any permissions they apply to files or folders they control.
- No sharing**:** Staff, pupils, parents, visitors and volunteers must **not** disclose account or password information. Breaches may result in disciplinary action and/or withdrawal of access.
- Issuing & resets**:** Initial credentials are issued by IT and must be changed on first login. Staff may request **password resets** for pupils where necessary; staff passwords are reset by IT on request.
- Changes & lockout**:** Users must change passwords when prompted, after a suspected compromise, or when instructed by IT. Devices must be **locked or logged off** when unattended.

13.2 Encryption & Use of Personal Devices

- School devices**:** School-owned devices and systems use appropriate encryption and security controls. Users must not attempt to disable or circumvent these protections.
- Personal devices**:** Staff may only access school data off-site or use personal devices (e.g., laptops, phones, USB media) where **explicitly authorised** and

only if those devices meet the School's security and encryption requirements. Authorisation and security standards are set by IT.

13.3 **Updates & Protection**

- Updates & anti-malware**:** School devices that support security updates, operating-system patches and anti-malware will have these installed and configured to update regularly or automatically.
- Safeguards**:** Users must not attempt to bypass, weaken or interfere with any technical, physical or administrative safeguards that protect personal data and the School's ICT facilities.
- Personal devices on the network**:** Any approved personal device connected to the School's network must meet the same security baseline (e.g., updates, encryption, anti-malware) and be configured in line with IT guidance.

14. Generative AI

14.1 **Purpose & Principles**

The School recognises the opportunities and risks presented by artificial intelligence (AI), including generative AI tools. In line with the DfE's guidance on AI in education, we use AI safely, ethically and transparently, ensuring compliance with safeguarding law, data-protection legislation, equality duties, and the School's educational aims.

Our use of AI follows the national regulatory principles of:

- safety and security,
- transparency,
- fairness,
- accountability,
- contestability

We retain human oversight at all times, AI may support decision making but must not replace professional judgement. This section applies to all staff, pupils, governors and volunteers using AI tools (including chatbots such as ChatGPT, Google Gemini and similar platforms).

14.2 **Safe and Responsible Use (Staff & Governors)**

Staff may use AI tools to support teaching, planning, resource creation, administration and workload reduction, provided they:

- Understand whether a tool is open (data used for training) or closed (data protected).
- Do not enter personal or sensitive data into open AI tools.
- Apply accuracy checks, fact-checking and scrutiny for bias.
- Attribute AI-generated outputs clearly where used.
- Ensure all content meets safeguarding, professional, legal and ethical standards.
- Staff must always consider whether AI is the appropriate tool for the task and remain professionally accountable for all outputs generated using AI.

14.3 **Staff Use**

Examples of appropriate use include:

- Drafting lesson materials, explanations, templates or resources
- Supporting planning and reducing workload
- Creating examples, analogies or model answers
- Drafting non-personal administrative documents
- Exploring alternative ways to differentiate or adapt learning materials

AI outputs must always be checked for accuracy, fairness, appropriate tone, and suitability for pupils before use in the classroom.

14.4 **Pupil Use**

Pupils may use AI only when explicitly permitted by staff, and only for age appropriate educational activities. Acceptable uses may include:

- Brainstorming or refining ideas
- Planning research questions
- Comparing or evaluating model examples
- Developing understanding of how AI works and its limitations

Pupils must reference the use of AI where it has been used to support work, using clear notation (e.g. “Generated using [tool], [date]”).

14.5 **Prohibited Uses (Pupils)**

AI must not be used to:

- Complete any summative assessment, exams, coursework or homework where AI generated content would constitute malpractice
- Pass off AI generated text or imagery as original work
- Generate content that is explicit, discriminatory, harmful, threatening or inappropriate
- Impersonate others, bully, harass or target individuals
- Circumvent filtering, monitoring or safeguarding systems

Unattributed AI use by pupils will be treated as plagiarism or academic misconduct in line with School assessment procedures.

14.6 **Safeguarding & Online Safety**

AI use can create safeguarding risks (e.g., harmful content, sexualised imagery, radicalisation, extortion, online contact risks). Any safeguarding concern arising from AI use must be reported immediately to the Designated Safeguarding Lead and managed under the Child Protection Policy. AI tools used in school remain subject to the School’s filtering & monitoring systems.

14.7 **Data Protection & Privacy**

In accordance with UK GDPR and the DfE’s AI and data protection guidance:

- Staff and pupils must not input personal data into open AI tools.
- Uploading personal data to a nonapproved AI system constitutes a data breach and will be managed under the Data Protection Policy.

14.8 **Assessment Integrity**

The School follows the latest Joint Council for Qualifications (JCQ) guidance on AI in assessments and takes all reasonable steps to prevent AI related malpractice.

AI may not be used for exam preparation, coursework, controlled assessments or any assignment where independent work is required.

14.9 **Training & Education**

The School provides ongoing training to ensure:

- Staff understand AI benefits, limitations, risks and professional responsibilities
- Pupils receive age-appropriate education on AI, including critical evaluation, bias, misinformation and online safety
- Governors are aware of their oversight obligations

AI-related training is embedded within staff safeguarding, online safety and digital-literacy development.

15. WiFi Access

15.1 **Purpose of the School WiFi Network**

The School's WiFi network is provided to support safe and efficient teaching, learning and school operations. All users must use the network responsibly and in accordance with this Policy and the relevant Acceptable Use Agreements.

15.2 **Network Security**

The School's WiFi is protected by secure authentication, content filtering and monitoring systems. Security settings and access controls are managed centrally by the ICT Network Manager.

Users must not attempt to bypass, alter or disable any filtering, monitoring, firewall or security controls applied to the WiFi network. Devices connected to the WiFi must be kept up to date with required security patches, anti-virus protection and encryption standards (as outlined in Section 13).

15.3 **Access for Pupils**

Pupils may connect only School-managed devices (e.g. 1:1 laptops) to the WiFi. Personal devices may not be connected unless authorised under a specific programme (e.g. BYOD arrangements for Sixth Form, if applicable). Pupil access is filtered, monitored and restricted to ensure age-appropriate and safe online activity.

15.4 **Access for Staff**

Staff may connect School devices to the staff WiFi network. Personal devices may only be connected where authorised and where they meet the School's security requirements.

Staff must ensure that no school data is accessed or stored on an unauthorised or unsecured personal device (see Section 13).

15.5 **Visitors and Contractors**

Visitors may be provided with temporary WiFi access at the discretion of the School.

Visitor access is restricted, monitored and separate from staff/pupil networks. Visitors must not access or attempt to access School systems, servers or restricted services via the WiFi network.

15.6 **Acceptable Use**

All use of the WiFi must comply with the School's Acceptable Use expectations (Sections 10, 11 and 12), including prohibitions on harmful, illegal or inappropriate online activity.

The School reserves the right to monitor and log usage on all WiFi networks for safeguarding, security and operational purposes. Misuse of the WiFi may result in removal of access rights, disciplinary action, or safeguarding or criminal referral where appropriate

15.7 **Reporting Issues**

Users must report any of the following immediately to the ICT Network Manager or DSL (as appropriate):

- Inappropriate or harmful content accessed on the network
- Concerns about cybersecurity, device compromise or unusual network activity
- Mistaken access to blocked or high-risk sites
- Any safeguarding concerns relating to online behaviour

16. Governance, Review & Quality Assurance

The policy is reviewed annually or sooner following any significant safeguarding incident or regulatory update, to ensure it remains compliant and effective.

The DSL and ICT Manager maintain regular logs of online safety events, monitoring alerts and technical issues, reviewing these together to identify emerging patterns or risks.

Reports provided to the Governing Body routinely include updates on monitoring alerts, filtering performance tests, AI-related incidents and cyber-security matters, reflecting statutory expectations around filtering, monitoring and safeguarding oversight.

Quality assurance processes include audits of curriculum coverage, checks on staff training compliance, risk assessments and ongoing selfevaluation against the DfE Digital & Technology Standards, ensuring the school continually develops its digital safeguarding provision.

Appendix A - Filtering & Monitoring Oversight Statement

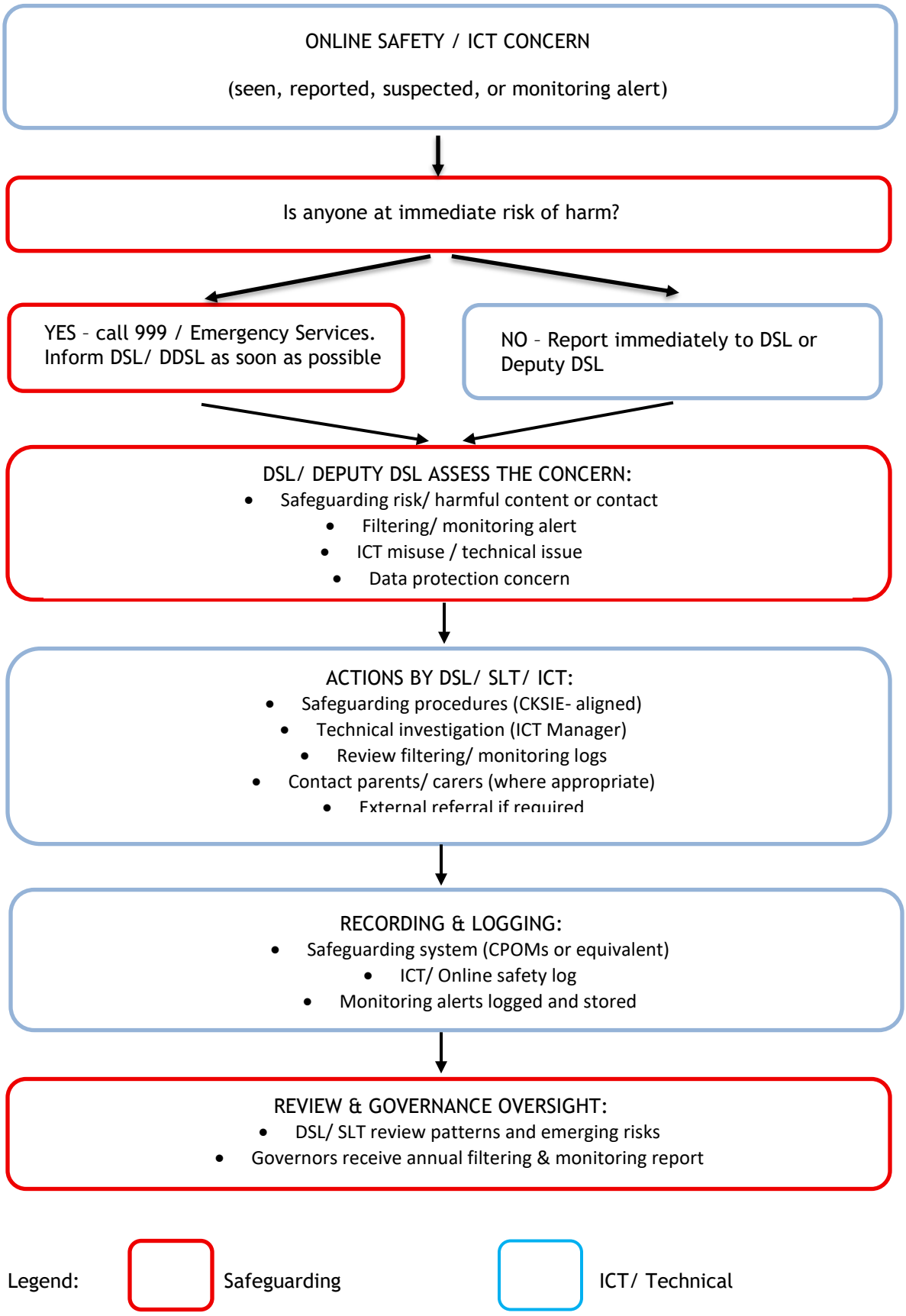
The School meets the DfE's *Filtering & Monitoring Standards* and ISI safeguarding requirements. The following arrangements are in place:

1. **Systems Used**
   - **Filtering provider:** *Smoothwall*
   - **Monitoring tools:** *Smoothwall Monitor, Classroom.cloud*
   - **Network protection:** Firewalls, anti-malware, secure configuration.

2. **Responsibilities**
   - **DSL:** Reviews monitoring alerts, responds to safeguarding concerns.
   - **ICT Network Manager:** Maintains filtering/monitoring systems, conducts technical testing, keeps logs.
   - **SLT:** Oversees effectiveness and implementation.
   - **Governors:** Receive an annual report and ensure systems meet DfE standards.

3. **Testing & Review**
   - Filtering is tested periodically using the SWGfL Test Page.
   - Monitoring alerts are reviewed daily (term time).
   - Systems are formally reviewed annually or sooner if risks change.
   - All incidents are recorded and reviewed through safeguarding procedures.

Appendix B - Flow Chart: Reporting Online Safety Concerns



Appendix C - Glossary

AI (Artificial Intelligence): Computer systems that generate predictions, content or decisions.

Closed AI tool: An AI system where data entered is not used to train public models.

Open AI tool: Public systems where input may train or be stored by the provider.

Content filtering: Technology restricting harmful or inappropriate online content.

Monitoring: Active supervision of online activity to detect risk.

DPIA: A Data Protection Impact Assessment used before adopting new tools.

Four areas of online risk: Content, Contact, Conduct, Commerce (DfE/KCSIE).

Malware: Malicious software designed to damage or disrupt systems.

VPN: Secure connection commonly used for remote access.

1:1 Device: A school-issued personal learning device such as a laptop or tablet.

Appendix D - Device Care & Security Checklist

For Staff & Pupils

- Keep devices in their protective case at all times.
- Never leave devices unattended in unsecured areas.
- Do not store food or drink near devices.
- Ensure the device is shut down or locked when not in use.
- Bring devices fully charged each day.
- Report faults or damage immediately to the ICT Support Team.
- Do not install or remove software.
- Never attempt repairs yourself.
- Keep the device away from extreme heat or cold.
- Use only school-approved chargers and accessories.
- Save work to the approved cloud location (OneDrive).
- Never share passwords or allow others to use your device.

Appendix E - WiFi Access Rules

Pupils

- Only School-managed devices may connect to pupil WiFi.
- All usage is filtered and monitored.
- Personal devices may not connect unless specifically authorised.
- Access is for educational use only.

Staff

- School devices may connect to staff WiFi.
- Personal devices may connect only with prior authorisation and must meet encryption/security requirements.
- Staff must not hotspot or share access with pupils.

Visitors / Contractors

- Visitor WiFi may be provided on request.
- Access is restricted and monitored.
- Visitors must not attempt to access school systems or pupil data.
- Use must comply with the Visitor/Volunteer AUA.

POLICY CONTROL – ICT & ONLINE SAFETY POLICY

Status & Review

Statutory policy or document	Yes
Publish on school website	Yes
Review frequency	Annually
Approval date	May 2026
Review date	May 2027

Version Control

Author	Creation / Revision Date	Version	Status
COO (MAD)	May 2026	**1.0**	Final approved version for publication. Complete re-write of previous policies: a) 1:1 Device Responsible Use Policy, b) BYOD Policy (Terms and condition, staff and visitors, wireless), c) iPad User Agreement and Acceptable User Policy, d) Online Safety Policy, e) Responsible Use of the Computer Network Policy, f) School rules for responsible use of the School's computer network, g) Staff Code of Conduct for Use of the Computer Network, h) Wireless Network Terms & Conditions. Introduction of version control