The Maynard School, Exeter

Sep 2025

6.24 Maynard School e-Safety Policy

Independent Day School for Girls

(This policy contains the Acceptable Computer Use Agreement (staff), and Acceptable Computer Use Policy for Students.)

This policy should be read and understood in conjunction with:

- The Maynard School AUP documents
-The Maynard School Child Protection and Safeguarding Policy
- Department for Education (DfE), Keeping Children Safe in Education (KCSIE) 2025
- DfE, Filtering and Monitoring Standards (September 2023, updated 2024)
- Working Together to Safeguard Children (HM Government, 2023)
- Counter-Terrorism and Security Act 2015 (Prevent Duty, Section 26)
- UK Council for Internet Safety (UKCIS), Education for a Connected World framework ProjectEVOLVE (SWGfL, UK Safer Internet Centre)

1. Purpose and Scope

The Maynard School is committed to safeguarding and promoting the welfare of all students. This E-Safety Policy sets out the school's approach to ensuring that children and young people are protected from risks associated with digital technologies. The policy applies to all members of the school community, including pupils, staff, governors, parents, contractors, and visitors. The school also aims to foster resilience and responsible digital citizenship, ensuring pupils are equipped to navigate an ever-changing digital landscape safely and responsibly.

The policy is aligned with statutory requirements including Keeping Children Safe in Education (2025), the Department for Education Filtering and Monitoring Standards, and relevant data protection legislation.

2. Roles and Responsibilities

• ***Designated Safeguarding Lead (DSL):*** Holds lead responsibility for online safety, supported by deputies and the Online Safety Lead (OSL).
• ***Online Safety Lead (OSL):*** Manages the operational implementation of e-safety strategy, reporting directly to the DSL.
• ***Governing Body:*** Provides strategic oversight, approves the policy, and ensures sufficient resources are allocated.
• ***All Staff:*** Expected to act as role models in their use of technology, follow the Acceptable Use Policy, and report safeguarding concerns.
• ***Students***: Required to use technology responsibly, follow age-appropriate guidance, and report concerns via school reporting systems.
• ***Parents/Carers:*** Encouraged to support the school's approach, follow guidance, and reinforce safe practice at home. The DSL and OSL must undertake regular, accredited training in online safety to remain up to date.

3. Key Principles

The school's e-safety strategy is based on the following principles: The policy also recognises that safeguarding responsibilities extend to incidents that occur outside of school where pupils' welfare is at risk, in line with *Keeping Children Safe in Education*.

• **Filtering and Monitoring:** The school uses *Securly* to filter and monitor internet use. Logs are reviewed weekly by the DSL and IT Manager, with incidents escalated through CPOMS where appropriate.
• **Reporting and Responding**: A clear incident flowchart is in place. The *Whisper*

anonymous reporting tool and other reporting mechanisms are available to pupils, staff, and parents.

- **Education and Training**: Online safety is taught through ICT and PSHE across all key stages. Staff receive training at induction and regular updates. Governors are encouraged to attend online safety training.
- **Professional Standards:** Staff must use only approved communication platforms and uphold the highest standards of professional conduct online.
- **Data Protection:** The school complies with GDPR and Data Protection legislation, overseen by the Data Protection Officer (DPO).

4. Policy Review and Oversight

This policy will be reviewed annually each June by the DSL and Online Safety Group, with formal approval by the Governing Body. It forms part of the wider safeguarding framework and is cross-referenced with policies including Safeguarding, Acceptable Use, Behaviour, Anti-Bullying, SEND, and Data Protection. The Online Safety Group, which includes governor will oversee implementation and monitor impact.

Appendices

Appendix A: Online Safety Action Plan (360 Safe Report)

The Maynard School has completed a comprehensive review using the 360 Safe framework. Key areas include responsibilities, policy development, professional standards, acceptable use, reporting and responding, staff training, governor involvement, parent engagement, filtering, monitoring, and technical security. The action plan identifies strengths such as strong leadership, robust filtering, integration into PSHE, and areas for development such as extending parental involvement, governor training, and refining monitoring systems.

The report can be found here: Action Plan Report.pdf and is regularly reviewed.

Appendix B: Reporting and Responding - Incident Response Flowchart

Reporting and responding

The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for schools to understand that reporting systems do not always respond to the needs of learners. While the report looks specifically at harmful sexual behaviours, schools may wish to address these issues more generally in reviewing their reporting systems. The Ofsted review suggested:

> *"School and college leaders should create a culture where sexual harassment and online sexual abuse are not tolerated, and where they identify issues and intervene early to better protect children and young people. ..In order to do this, they should assume that sexual harassment and online sexual abuse are happening in their setting, even when there are no specific reports, and put in place a whole-school approach to address them. This should include:*
>
> - *routine record-keeping and analysis of sexual harassment and sexual violence, including online, to identify patterns and intervene early to prevent abuse"*

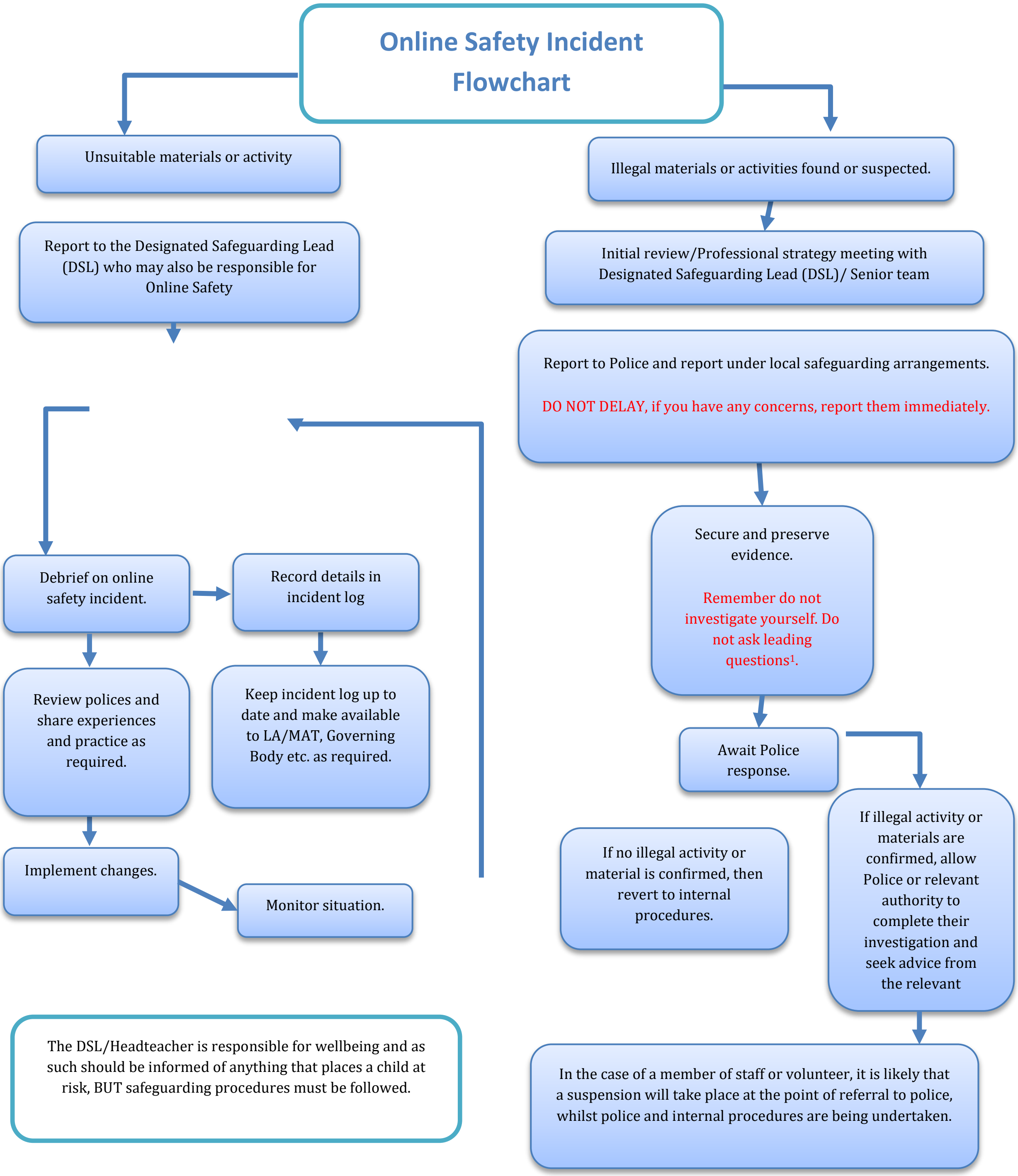
The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- **there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.** (Schools may wish to consider the use of online/anonymous reporting systems, which can be used by all members of the school community e.g. SWGfL Whisper)
- **all members of the school community will be made aware of the need to report online safety issues/incidents**
- **reports will be dealt with as soon as is practically possible once they are received**
- **the Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.**
- **if there is any suspicion that the incident involves any illegal activity or the potential for serious harm** (see flowchart and user actions chart in the appendix), **the incident must be escalated through the agreed school safeguarding procedures, this may include**
  - Non-consensual images
  - Self-generated images
  - Terrorism/extremism
  - Hate crime/ Abuse
  - Fraud and extortion

    - Harassment/stalking
    - Child Sexual Abuse Material (CSAM)
    - Child Sexual Exploitation Grooming
    - Extreme Pornography
    - Sale of illegal materials/substances
    - Cyber or hacking offences under the Computer Misuse Act
    - Copyright theft or piracy
- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority / MAT
- where there is no suspected illegal activity, devices may be checked using the following procedures:
    - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
    - conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
    - ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
    - record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form
    - once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
        - internal response or discipline procedures
        - involvement by local authority / MAT (as relevant)
        - police involvement and/or action
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents should be logged (insert details here). (A template reporting log can be found in the appendix, but many schools will use logs that are included with their management information systems (MIS).
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant)

- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
  - *the Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with*
  - *staff, through regular briefings*
  - *learners, through assemblies/lessons*
  - *parents/carers, through newsletters, school social media, website*
  - *governors, through regular safeguarding updates*
  - *local authority/external agencies, as relevant (The Ofsted Review into Sexual Abuse in Schools and Colleges suggested "working closely with Local Safeguarding Partnerships in the area where the school or college is located so they are aware of the range of support available to children and young people who are victims or who perpetrate harmful sexual behaviour"*

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



Online Safety Incident Flowchart

Unsuitable materials or activity

Report to the Designated Safeguarding Lead (DSL) who may also be responsible for Online Safety

Debrief on online safety incident.

Record details in incident log

Review polices and share experiences and practice as required.

Keep incident log up to date and make available to LA/MAT, Governing Body etc. as required.

Implement changes.

Monitor situation.

The DSL/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.

Illegal materials or activities found or suspected.

Initial review/Professional strategy meeting with Designated Safeguarding Lead (DSL)/ Senior team

Report to Police and report under local safeguarding arrangements.

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

Secure and preserve evidence.

Remember do not investigate yourself. Do not ask leading questions[1].

Await Police response.

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

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

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

Appendix C: Acceptable Use Agreements

All staff, students, and parents are required to sign Acceptable Use Agreements before accessing the school's IT systems. These agreements set out expectations for responsible use, data protection, communication, and sanctions for misuse. Age-specific versions are in place for younger students, with explicit parental consent required for internet and device use.

Student Acceptable Use Agreement for KS2 – KS5 students

Maynard School Policy

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

This Acceptable Use Agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the Maynard School will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the Maynard School systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the Maynard School systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal devices (mobile phones / USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any

programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

- I will immediately report any damage or faults involving equipment or software; however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will not use social media sites in school

When using the internet for research or recreation, I recognise that:

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

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

- I understand that the Maynard School also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Bring Your Own Device Agreement

This agreement document applies to students who bring their own digital devices into school for educational purposes only. Such devices will be used in lessons by students when given express permission by their teacher to enhance learning. The school is allowing the device on the network and internet through our Wi-Fi access points.

Currently, L5 to U6 students are allowed to bring an iPad or laptop to lessons.

Students with digital devices being connected to the Maynard School network have to agree to the following conditions:

- Students will be restricted to one allowed device per person.
- Digital devices are subject to the school's "mobile phones and other electronic devices policy" and should remain switched off and in bags unless permission is given to use them

during the school day. Students not in the sixth form should not use be using their own devices at break and lunch times unless engaged in supervised work e.g. in the library.

- Digital devices may be confiscated at any time for inappropriate use. Under the 2011 Education Act, the school retains the right to search digital devices and examine the data and files on the device (see Searching Student's Policy)
- ICT support will be only be given for personal digital devices at the discretion of the Network Manager or teacher.
- Digital Devices should not be connected to the school's peripherals such as printers, speakers or projectors.
- The charging of digital devices at school is not permitted. Devices should be fully charged at home with sufficient free memory to be able to engage in educational activities within lessons.
- Up-to-date antivirus software and all additional software updates must be installed where appropriate.
- Students will be responsible for the security and protection of personal digital devices. The school accepts no responsibility for loss or damage to personal digital devices. Devices should be covered by parents' home insurance. Students should be conscious of personal safety when carrying digital devices to, around and from school.

Agreement in relation to remote learning and associated platforms

It may be that in times of closure or remote learning the school requires you to use a variety of platforms to engage in distant learning. These are the rules to follow to safeguard yourselves in such instances:

- Do not share your online access usernames or passwords with anyone else.
- Do not copy links to private or limited access in school videos with anyone outside the school community.
- Only show your webcam when required by the teacher for that episode of the lesson (and if you feel comfortable in doing so).
- Only show your screen or desktop when required by the teacher for that episode of the lesson (and if you feel comfortable in doing so).
- Only use your microphone when required by the teacher for that episode of the lesson (and if you feel comfortable in doing so).
- If showing work or presenting on webcam ensure that you are appropriately dressed.
- If showing work or presenting on webcam ensure that any background location / image is appropriate.
- If you are contributing to the lesson with your microphone on please use appropriate language and be aware of any other background noise in the vicinity.
- Do not record any part of the lesson or share any school related folders, files or resources without prior permission.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Student Acceptable Use Agreement Form

This form relates to the student Acceptable Use Agreement, to which it is attached.

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

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

- I use the Maynard School systems and devices (both in and out of school)
- I use my own devices in the Maynard School (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I use my own equipment out of the Maynard School in a way that is related to me being a member of this Maynard School e.g. communicating with other members of the school, accessing school email, VLE, website etc.

Name of Student: --

Form / Class: --

Signed: --

Date: --

Parent / Guardian Countersignature: --

Digital Device brought to school (if applicable – e.g. iPad Air 16GB):……………………..…………...

Student Acceptable Use Policy Agreement for KS1 Students

This is how we stay safe when we use computers:

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

Signed (child): --

Signed (parent): --

Staff (and Governor / Volunteer) Acceptable Use Policy Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

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

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

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the Maynard School will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school. (schools should amend this section in the light of their policies which relate to the personal use, by staff and volunteers, of school systems)
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using Maynard School ICT systems:

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

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

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using Maynard School equipment. I will also follow any additional rules set by the Maynard

School about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

- I will not use personal email addresses on the Maynard School ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant Maynard School policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in Maynard School policies.
- I will not disable or cause any damage to Maynard School equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Maynard School eSafety Policy, Data Protection Policy and Data and Document Retention Policy'. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by Maynard School policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

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

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

When using the internet in a professional capacity at home or during remote learning situations I will:

- Always use school accounts and platforms to communicate with the students.
- Consider appropriateness of language, wardrobe and location and be aware of background noise and video at all times.
- Avoid one on one meetings or sessions. If this is unavoidable then invite other staff in the department, myself and SLT line manager into the session too this is essentially like teaching with an open door. Moreover, if one on one, make sure you record the session.
- Before recording any session alert the students to this fact and ensure you get permission. This may impact upon whether they wish to respond to questions or use their web cam feature.
- Before inviting any student to share webcam or recording or desktop just remind them to consider whether they are in appropriate wardrobe / locations and whether the screen would be appropriate to share.
- Remind students to not record any part of the lesson themselves or to share private links or videos anywhere outside the school community.
- If the lesson doesn't really require 'live' elements or webcams or microphones etc then don't use them.
- The webcams of students shouldn't remain on throughout the lesson, only when required and they are invited to do so. Same goes for microphones.
- We are not using 'Zoom' at present. It is not a secure Microsoft365 or linked school platform and there are privacy issues which have been widely reported.
- I'd invite your HoD or an SLT member into each Microsoft Teams chat and group you have - essentially creating an open-door effect.
- Don't share or comment on any private / confidential information on any online platform.

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

- I understand that this Acceptable Use Policy applies not only to my work and use of Maynard School digital technology equipment in school, but also applies to my use of Maynard School systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and in the event of illegal activities the involvement of the police.

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

Staff / Governor / Volunteer Name: --

Signed: --

Date: --

Appendix D: Filtering and Monitoring Technical Guidance

The school uses *Securely* to filter and monitor online activity across all school-owned and BYOD devices. Logs are reviewed weekly by the DSL and IT Manager, and alerts are escalated immediately for safeguarding concerns. Filtering is differentiated by age and role. BYOD access is monitored, and visitor Wi-Fi is safeguarded. Annual reviews of filtering and monitoring effectiveness are carried out, overseen by governors.

Appendix E: Online Safety Curriculum

Online safety education is delivered from Year 1 to Year 9 through ICT and PSHE lessons. Topics include cyberbullying, grooming, online gambling, radicalisation, social media, and digital footprints. Resources are mapped against Project Evolve and the UKCIS Education for a Connected World framework. Lessons are regularly updated to reflect emerging risks such as AI, influencers, and online extremism.

Appendix F: Data Protection and GDPR

The school complies with the Data Protection Act 2018 and GDPR requirements. A Data Protection Officer (DPO) oversees compliance, data audits, and subject access requests. Staff are trained in secure data handling, encryption, and two-factor authentication. Policies cover data storage, sharing, disposal, and the use of cloud services. Consent is sought for non-core activities such as digital images. AI use in education is assessed for data protection impact.

Appendix G: Governor and Parent Engagement

Governors: The governing body approves this policy and receives regular reports on online safety. At least one governor is a member of the Online Safety Group and is encouraged to attend training provided by SWGfL or the UK Safer Internet Centre.

Parents: The school engages parents through newsletters, website resources, and information sessions. A Childnet workshop was held in April 2025. Parents are encouraged to support safe online behaviours at home and to use the Whisper reporting system for concerns.

Appendix H: Social Media Guidance

The school provides clear expectations for staff and student use of social media in the code of conduct documents. Staff must not use personal social media accounts to contact students or parents. Students are taught about the risks of social media, including cyberbullying, reputation management, and safe online communication. Social media platforms are restricted on the school network but are addressed through the curriculum.

Appendix I: Mobile Technology and Devices

The school operates a secure device lease / BYOD scheme for Sixth Form students, with plans for phased rollout. All devices are subject to Securly monitoring when connected to the school network. Clear expectations for staff, students, and visitors are outlined in the

Mobile Technology Policy. Visitors receive safeguarding information including rules for device use.

Appendix J: Digital Images and Video Guidance

The school has a clear Digital Images and Video Policy, requiring parental consent before using student images in publications. Staff must use only school-authorised devices for capturing images, or must have permission from senior staff that is risk assessed. Images must be stored securely and disposed of in line with GDPR requirements. Guidance is provided to staff, students, and parents on the safe creation, use, and sharing of digital media.

Written by JF/PR	June 2018
Updated by ML	June 2025
Approved by Govs	xxxx
Review date	June 2026