

The Mortimer Federation of St John's and St Mary's

Internet Access and E-Safety Policy			
Committee	Curriculum	Date of Issue	June 2023
Status		Review Date	June 2026
		Issue Number	2

THE MORTIMER FEDERATION OF ST. JOHN'S AND ST. MARY'S

INTERNET ACCESS AND E-SAFETY POLICY

Introduction

The National Curriculum requires pupils to use Information and Communications Technology (ICT) which may include web-based resources and e-mail. The purpose of this document is to outline how this technology will be accessed by pupils and staff at The Mortimer Federation of St. John's and St. Mary's, and to identify the measures that are in place to protect all users from access to inappropriate material.

1. Background

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. ICT is an essential resource to support learning and teaching, and plays an important role in the everyday lives of children, young people and adults. Schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment, and ensure safe and appropriate use of ICT resources.

The internet is not consistently policed. All users need to be aware of the range of risks associated with the use of internet technologies, for example:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of/sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying
- Access to age inappropriate video/internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism, copyright Artificial Intelligence infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies).

The school must demonstrate that it has done everything that could reasonably be expected of it to manage and reduce these risks. Although this policy concerns the use of computing and communications technology, e-safety is not purely a technical issue – it should be managed within the context of child welfare and safeguarding. The school will also help to educate parents as to the risks of using the internet, such that e-safety is promoted outside of the school, where children may have more unrestricted use of the internet.

2. Scope

This policy applies to all members of the school community (including staff, students/pupils, volunteers, governors, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

Both this policy and the Acceptable Use Policies (for all staff, governors, volunteers, visitors, contractors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, iPads,

The Mortimer Federation of St John's and St Mary's

Internet Access and E-Safety Policy			
Committee	Curriculum	Date of Issue	June 2023
Status		Review Date	June 2026
		Issue Number	2

whiteboards, digital video equipment, etc.) and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, smart phones, tablets, smart watches, etc).

3. Reasons for accessing the internet using School network provision

Use of the Internet is cross curricular and at all ages with the primary curriculum there is demand for use of on-line resources and materials. Future developments will mean even greater emphasis on web-based resources.

The Internet, apps, virtual learning platforms, cloud-based systems, e-mail and other communications systems, if used correctly, will enhance school life by:

- Supporting and enhancing the staff in provision of the curriculum
- Extending the learning experience for pupils and teaching a range of important life skills
- Complementing the school's management information and business administration

3a. Pupil use

Pupils will only use the Internet under close staff supervision with the focus usually on prepared material. Access will normally be to educational sites that link to areas of the curriculum being delivered at the time. Internet use will therefore be self-limiting and appropriate to the user.

3b. Staff use

Staff will be allowed use specifically to support their work. Access to public chat rooms will not be allowed.

3c. Governor use

Governors will be allowed access to support their role as governor including access to local authority provision. No other access will be allowed.

4. Review Schedule

This policy will be reviewed every three years by the school's ICT subject leader in consultation with the ICT governor and safeguarding governors.

This policy will be updated by the school's ICT subject leader, the Safeguarding Governor and the ICT Governor when the school introduces significant new technology or ICT services that are not covered by the policy, or as a result of a review of e-safety incidents. The Curriculum Committee will approve the policy.

5. Roles and Responsibilities

Governors

The e-safety policy falls under the role of the Safeguarding Governor, who will:

- Meet regularly with the ICT subject leader;
- Monitor and review any e-safety incidents;
- Report e-safety status and compliance to the Governing Body in their Safeguarding capacity.
-

Also, support the school in encouraging pupils, family and the wider community to engage in online safety activities.

Ensure that the school is using appropriate filters and monitor systems to safeguard pupils but not lead to unreasonable restrictions that might limit pupils' online teaching and learning opportunities.

The Mortimer Federation of St John's and St Mary's

Internet Access and E-Safety Policy			
Committee	Curriculum	Date of Issue	June 2023
Status		Review Date	June 2026
		Issue Number	2

Executive Headteacher

The Executive Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community and ensuring that online safety is integrated through all practice; although the day to day responsibility for e-safety may be delegated to a nominated ICT subject leader.

The duties of the Executive Headteacher in relation to e-safety are:

- To ensure all policies and procedures are followed by staff;
- Ensure all staff are trained in online safety and safeguarding and they know the procedures for reporting an e-safety incident;
- Ensure the school implements and uses effective ICT systems, including school-safe filtering and monitoring systems and protected email and cloud systems;
- Update governors on changes to the school's online safety procedures.

The Executive Headteacher (Designated safeguarding lead – DSL) and the deputy DSLs should be aware of the e-safety incident procedure detailed in this document to be followed in the event of a serious e-safety allegation being made against a member of staff.

ICT Subject leader

The duties of the ICT subject leader in relation to e-safety are:

- To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
- To liaise with the Local Authority;
- To liaise with school ICT technical staff;
- To collate and review e-safety incidents to inform future e-safety developments;
- Report termly to Senior Leadership Team;
- To review and update this policy and other online safety documents (e.g. acceptable use policies);
- Keep up to date with online safety issues;
- Ensure that the teaching of online safety is embedded throughout the curriculum and beyond, in wider school life;
- Promote online safety to parents and the wider school community;
- Facilitate training and advice for staff.

Procedures to be followed in the event of an e-safety incident

In the event of an e-safety incident follow steps on the flow chart in Appendix 1 and follow the normal safeguarding procedures:

All incidents would also be logged using one or more of the following school procedures: safeguarding, GDPR or CREST, dependent on the particulars of the incident. The DSL feeds back any e-safety safeguarding concerns to the safeguarding governor termly.

Network Manager (provided through a range of third party ICT support and internal ICT technician)

- To provide a technical infrastructure to support internet safety practices – for example, effective filtering, monitoring, firewall, and virus protection;
- Ensure stakeholders understand the consequences of existing services and of any changes to the system.
- To provide sufficient log and audit information to allow the ICT subject leader/Executive Headteacher to satisfy themselves that the school's network provision is not being misused;
- To report breaches of acceptable use of ICT facilities to the ICT subject leader/Executive Headteacher.
- Manage the school's systems, networks and devices, according to strict password policy, adequate protection encryption and backup for data.

The Mortimer Federation of St John's and St Mary's

Internet Access and E-Safety Policy			
Committee	Curriculum	Date of Issue	June 2023
Status		Review Date	June 2026
		Issue Number	2

Teaching and Support staff

Are responsible for ensuring that staff:

- Have an up to date awareness of e-safety matters and of the current school e-safety policy and practices;
- Have read, understood and signed the school Staff Acceptable Use Policy (AUP),
- They ensure pupils never have unsupervised access to the internet;
- Whenever overseeing the use of technology (devices, the internet, etc.) in school or setting as homework tasks, encourage sensible use, think about any potential dangers, monitor what pupils/students are doing carefully and consider the age appropriateness of websites;
- They guide pupils in critical thinking in their use of online materials (e.g. fake news, copyright, etc);
- They ensure pupils log off apps and devices once they have finished using them;
- They prepare and check all online resources and sources before use.
- They report any suspected misuse or problem to the ICT Subject leader for investigation.
- They understand that online safety is a core part of safeguarding and is everyone's responsibility.
- Online-safety incidents should be recorded in the same way as any safeguarding incident.
- They identify opportunities to thread online safety through all school activities, both inside and outside of the classroom and within the curriculum.
- They model safe, responsible and professional behaviours in their own use of technology; both in school and out (see social networking policy for further guidance).

6. Policy Statements

Acceptable Use

It is expected that at all times the use of ICT equipment, facilities, and resources will be made by all users in strict compliance with the Acceptable Use Policy which they have signed.

No person will be permitted to use school ICT resources without first agreeing and signing an Acceptable Use Policy appropriate to the intended use.

Pupils

A planned e-safety programme should be provided as part of ICT/PSHE/other lessons and should be regularly reviewed to ensure it is up-to-date with respect to new technologies in school and outside school.

Pupils will be taught what Internet use is acceptable and what is not and given clear guidelines for Internet use.

Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.

At no time will pupils be permitted to access the Internet without close supervision from a member of staff.

Pupils are not permitted to download programs or files onto school based technologies.

Parents/Carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of their children's on-line experiences.

The Mortimer Federation of St John's and St Mary's

Internet Access and E-Safety Policy			
Committee	Curriculum	Date of Issue	June 2023
Status		Review Date	June 2026
		Issue Number	2

The school will therefore provide information and awareness to parents and carers through the school's website, directing them to key websites that provide detailed guidance on e-safety issues. The school will also regularly send home information on e-safety issues for parents and provide training opportunities.

The school will collaborate with other local schools to publicise e-safety guidance and awareness events.

Teaching and Support Staff

New staff will receive information on the school's Acceptable Use Policy as part of their induction.

All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.

All staff are encouraged to incorporate e-safety activities and awareness within their curriculum areas.

An audit of the e-safety training needs of all staff will be carried out annually.

Staff are not permitted to download programs or files onto school-based technologies without obtaining prior permission from the ICT subject leader.

Staff may not use personal removable media such as USB memory sticks or portable disk drives on school equipment. The school provides secure, encrypted memory sticks; if staff require additional capacity they may request extra memory sticks from the ICT subject leader.

Governors

Governors should ensure that they remain conversant with e-safety issues. This is particularly important for those who are members of any sub-committee or group involved in ICT, e-safety, health and safety, or child protection. There may be several sources of information for governors, for example:

- Reading the materials available on the West Berkshire Governors' Services website;
- Attendance at training provided by the Local Authority, National Governors Association, or other relevant organisation;
- Participation in school training and information sessions for staff or parents.

Governors are not permitted to download programs or files onto school based technologies without obtaining prior permission from the ICT subject leader

Technical – equipment, filtering, and monitoring

7. Technical framework:

Mortimer St. John's

Mortimer St. John's Internet Service Provider (ISP) is operated by BT via Elmdale. This means that the school accesses the Internet through a safe and secure environment. The school has a local server based on site. The email system is provided by Microsoft using the Office365 platform and is hosted in Microsoft datacentres.

Securly Software is used as the primary filter to ensure inappropriate sites are not reached. Filtering is ongoing but in the unlikely event that material found by users is deemed unsuitable it can be reported to Bradfield College to be filtered out. There is also a substantial firewall in place to prevent mis-use of the Internet connection which is managed by Elmdale. Bradfield College oversees and manages the security

The Mortimer Federation of St John's and St Mary's

Internet Access and E-Safety Policy			
Committee	Curriculum	Date of Issue	June 2023
Status		Review Date	June 2026
		Issue Number	2

updates needed to keep the network secure. Bradfield College ensures that anti-virus protection is installed and kept up-to-date on all school machines.

Mortimer St. Mary's:

Mortimer St. Mary's has purchased its Internet connectivity from Gigaclear. The email system is provided by Microsoft using the Office365 platform and is hosted in Microsoft datacentres.

Securly is used as the primary filter to ensure inappropriate sites are not reached. Filtering is ongoing but in the unlikely event that material found by users is deemed unsuitable it can be reported to Bradfield College to be filtered out. There is also a substantial firewall in place to prevent mis-use of the Internet connection which is managed by Elmdale. Bradfield College oversees and manages the security updates needed to keep the network secure. Bradfield College ensures that anti-virus protection is installed and kept up-to-date on all school machines.

The Federation is responsible for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible, and use third party providers where required to achieve this. The school is also responsible for ensuring policies and procedures approved within this policy are implemented. Servers, wireless systems and cabling must be securely located and physical access restricted. All users will have clearly defined access rights to school ICT systems. All passwords for the management of the school ICT system are stored securely in Bradfield College's Last Pass system.

Using Digital Photographs, Video, and Sound recordings

Staff are allowed to take digital photographs, video images, or sound recordings to support educational aims, but must follow school policies concerning the sharing, distribution and publication of such material. All parents are requested to complete a photograph consent form authorising the use of such material.

Images or recordings may only be taken using school equipment; the personal equipment of staff must not be used for such purposes. However, with the express permission of the Executive Headteacher (for example, when on a school trip), images can be taken provided they are transferred immediately and solely to the school's network and then deleted from the staff device.

Digital photographs, sound recordings or videos of pupils, staff or work may only be stored on secure GDPR compliant systems. This includes the use of Seesaw as a cloud-based learning journal.

Visitors wanting to use personal portable media to share images/files (e.g. USB sticks) to deliver presentations, training, etc. must have permission from SLT or the School Office. Visitors will always be encouraged to send presentations/resources in advance of their visit.

Any pupils who bring phones onto the school premises have to hand them into the office as soon as they arrive and collect them at the end of the day. They are not allowed to use them at all within school.

The school does not use publicly accessible webcams. Webcams in school may only ever be used for specific learning purposes (for example, remotely monitoring a nesting box) and never using images of children or adults.

Parents will be reminded at least annually, about the importance of not sharing images of other peoples' children due to children protection reasons, when photos have been allowed at school events.

The Mortimer Federation of St John's and St Mary's

Internet Access and E-Safety Policy			
Committee	Curriculum	Date of Issue	June 2023
Status		Review Date	June 2026
		Issue Number	2

Video-conferencing

Videoconferencing enables users to see and hear each other in different locations. It is a 'real time' interactive technology and has many uses in education. Equipment ranges from small PC systems/iPads (web cameras) to large room based systems that can be used for whole classes or lectures. The videoconferencing equipment uses a 'network' to communicate with the other site.

Parents and carers will be informed in advance if their children are to be involved in video conferences with end-points outside the school (for example, to another school, or to an organisation providing educational support or services).

All pupils will be supervised by a member of staff when video conferencing.

The school will keep a record of video conferences, including date, time and participants.

Governors and staff may use video conferencing (Microsoft Teams) or remote calling as a means of holding meetings when all or some of the participants are unable to attend the meeting in person. The standard code of conduct for such meetings is expected. Staff may also conduct meetings with external professionals via video-conferencing or remote calls when necessary, using GDPR compliant systems.

No part of any video conference will be recorded in any medium by any participant without the consent of all those taking part.

Note: Participants in conferences offered by 3rd party organisations might not be DBS checked. Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

The Mortimer Federation of St John's and St Mary's

Internet Access and E-Safety Policy			
Committee	Curriculum	Date of Issue	June 2023
Status		Review Date	June 2026
		Issue Number	2

When personal data is stored on any portable computer system, USB stick or any other removable media:

- The data must be encrypted and password protected.
- The device must be password protected.
- The device must be checked for viruses or malware immediately on connection to school equipment.
- The data must be securely deleted from the device once it has been transferred or its use is complete.

Publishing Content

The school's website is designed to promote the school and publish resources to support pupils, parents and school life. The safety of information published on the website must be considered from a personal and school security viewpoint.

Photographs published on the website, or elsewhere, that include pupils will be selected carefully and will comply with GDPR requirements. Care should be taken not to include images of pupils who for any reason should not be publically identified i.e. parental consent not received.

Care should be taken when publishing digital photograph or video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

E-Mail

All users

It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced.

Pupils

Pupils may only use approved email accounts/messaging systems, under close supervision from a member of teaching staff and for educational purposes as approved by the Executive Headteacher. Only whole-class email addresses, monitored group emails or messaging systems direct with school adults (e.g. on Seesaw), within GDPR compliant platforms, will be used for all such approved communications.

Staff, Governors, Volunteers

All email communication concerning school business between school staff or governors and any individual or organisation must be conducted using school Microsoft Outlook365 email accounts. Under no circumstances should staff or governors conduct any school business using personal e-mail addresses.

Staff sending e-mails of a particularly sensitive nature, to external organisations or parents, are advised to cc. in the Executive Headteacher or their line manager. Emails to parents regarding pupils should always go through the school office. Staff should never email pupils.

Staff must immediately report to the Executive Headteacher the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

The Mortimer Federation of St John's and St Mary's

Internet Access and E-Safety Policy			
Committee	Curriculum	Date of Issue	June 2023
Status		Review Date	June 2026
		Issue Number	2

Social Networking Sites, Chatrooms, Instant Messaging

Staff and Governors must take great care when using any social networking facility, internet chatroom, messaging facility, or web log that they do not publish information or photographs relating to the school that is confidential, reflects upon the school in a derogatory or defamatory manner or will bring the teaching profession into disrepute. Messages and updates so published must not be offensive to colleagues or breach the integrity of the ethos of the school or bring the school into disrepute. It is also required that no comments or references are made relating to any current or former pupil of The Mortimer Federation of St. John's and St. Mary's using school derived or related social media systems.

Any referencing or commenting relating to The Mortimer Federation of St. John's and St. Mary's via the Facebook social networking system should only be done via the Executive Headteacher approved page or version of the site, to ensure compliance and relevance. The same process should apply to any similar social media forum or web page(s) used in the future.

Copyright

The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.

All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.

Dealing with Incidents

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure or, where appropriate, the West Berkshire Council Disciplinary Procedures.

Policy breaches may also lead to criminal or civil proceedings.

All incidents would also be logged using one or more of the following school procedures: safeguarding, GDPR or CREST, dependent on the particulars of the incident.

For the avoidance of doubt, activities that will cause an e-safety incident to be raised are given below.

Unsuitable, Inappropriate, but legal activities

The following Internet and email activities will not be tolerated on school ICT equipment or services, whether in school or outside. These activities while not illegal are considered by the school as unsuitable or inappropriate.

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- Pornography;
- Promotion of any kind of discrimination;
- Promotion of racial or religious hatred;
- Threatening behaviour, including promotion of physical violence or mental harm;

The Mortimer Federation of St John's and St Mary's

Internet Access and E-Safety Policy			
Committee	Curriculum	Date of Issue	June 2023
Status		Review Date	June 2026
		Issue Number	2

- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute.

Users may not:

- Run a private business using school ICT equipment, systems, or services;
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by West Berkshire Council or the school;
- Upload, download or transmit commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions;
- Reveal or publicise confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords);
- Create or propagate computer viruses or other harmful files;
- Carry out sustained or instantaneous high volume network traffic (e.g. downloading/uploading files) that causes network congestion and hinders others in their use of the internet;
- Play non-educational on-line games;
- Gamble on-line;
- Use school ICT equipment, systems, or services for Internet file sharing;
- Use social networking sites.

Illegal Activities

The following Internet and email activities are illegal and will not be tolerated on school ICT equipment or services, whether in school or outside.

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- Child sexual abuse images;
- Promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation;
- Adult material that potentially breaches the Obscene Publications Act in the UK;
- Criminally racist material in the UK;
- The promotion of terrorism.

8. Disclaimer

In school, Internet use will be supervised and all reasonable precautions taken to ensure unsuitable material is never found. If staff find unsuitable material it can be reported to the LA. These measures are in addition to the filtering and firewall prevention operated by the LA. Nevertheless, in the event that unsuitable material is accessed, neither the school nor West Berkshire Council can accept liability for the material or the consequences of the access.

9. Complaints

Complaints concerning Internet access will be handled under the Complaints Policy.

Chair of Curriculum Committee

Date

Share Your Light

John 10:10 "Life in all its fullness"

The Mortimer Federation of St John's and St Mary's

Internet Access and E-Safety Policy			
Committee	Curriculum	Date of Issue	June 2023
Status		Review Date	June 2026
		Issue Number	2

Appendix 1

