Marlborough School's Online Safety Policy

Last Reviewed: January 2026

Future Review date: January 2027

Signed:

Policy Title	Online Safety Policy
Policy Number	24
Date of Publication	March 2024
Author	Local Authority – adapted by Abigail Squibb

Date of Review	Amendments from previous version	Amended by	Approved by
March 2026		Abigail Squibb	FGB

What is Online Safety?
Online Safety enables us to make a proactive stance to ensure that the safest and most appropriate use of technologies are in place and thereby minimise any risks. Online Safety is used alongside other school safeguarding policies and applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of the school ICT systems, both in and out of school.

Why do we need Online Safety?

- to ensure that children and whole school community are safe and are protected from potential harm, both within and outside school

Significant educational benefits result from curriculum internet use, including access to information from around the world and the ability to communicate widely. Internet safety depends on staff, schools, governors, advisers, parents and carers to take responsibility for the use of the Internet.

Marlborough School has a duty to provide children with quality internet access as part of their learning experience.
The purpose of internet use in school is to:

- raise educational standards
- promote pupil achievement
- support the professional work of staff
- provide an audience for pupils' work
- develop pupils' skills and knowledge in order to use technology
- access to world-wide educational resources including museums and art galleries.

Staff will adopt an ethos to promote safe use to ensure that users only access appropriate material.
Pupils have regular reminders about rules, guidelines and useful information for internet access.
Virus protection is installed and updated regularly across the entire school. The ICT and internet facilities are available to all Marlborough School children, staff and Governors.

Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety
- Meeting digital and technology standards
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education (RSE) and health education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

How do we communicate and apply Online Safety?

Staff lead for Online Safety: **Martin Gimenez**
Link Governor for online Safety: **Ben Godsall**

- The Staff Lead for ICT and ICT support assistant (providing a safety net), discuss current issues, review incident logs and filtering/passwords, produce, review and monitor the-safety policies, attend and disseminate training sessions.
- The Online Safety officer and ICT support assistant regularly liaise with the ICT infrastructure support team to ensure the school's system is secure and is not open to misuse or malicious attack and that the school meets e-safety technical requirements.
- The Online Safety office and ICT support assistant receives regular safety updates through SWGRL and provides advice / guidance / training as appropriate to relevant parties:
    - Online Safety governor to the governing body
    - IT support assistant – general issues
    - Computing subject lead – curriculum issues
- Adults, pupils and parents adhere to the school acceptable use policy.
- Adults adhere to the user responsibilities (annex 2)
- Misuse guidance (annex 4), outlines the procedures in the event of an e-safety incident.
- Online safety issues are embedded in the curriculum; a planned online safety programme is followed in all classes as part of Computing and PSHE and is regularly revisited.
- Staff check websites for children's use and inform IT technician if any unsuitable material is found in internet searches.
- The school seeks to provide information and awareness to parents and carers e.g. newsletters, parent evenings, reference to websites e.g. SWGfL "Golden Rules" for parents.

Principles for Acceptable Use of the Internet
Use of school computers by pupils must be in support of the aims and objectives of the Primary National Curriculum.

Online activities which are encouraged include:
• Use of the internet to investigate and research school subjects, cross-curricular themes or topics.
• The development of pupils' competence in ICT skills and their general research skills.
• Use of the internet to support homework and further study.

Online activities which are <u>not</u> permitted include:
• Searching, viewing or retrieving materials that are not related to the aims of the curriculum.
• Copying, saving or redistributing copyright-protected material, without approval.
• Subscribing to any services or ordering any goods or services, unless specifically approved by the school.
• Playing computer games or using other interactive 'chat' sites unless specifically approved by the school.
• Using the network in such a way that disrupts/hinders other users (for example: downloading large files during peak usage times; streaming live sports/news feeds).
• Publishing, sharing or distributing any personal information about a user (such as: home address, email address, phone number etc).
• Downloading software without permission from the Schools Network Manager.
• Any activity that violates a school rule.

Guidance on the use of email
Anyone receiving an unwanted email should report it immediately to any teacher. Anyone caught sending such messages will have their access to the technology denied.

General Guidance for All Users
• Staff are encouraged to use ICT resources in their teaching and learning activities, to conduct research, and for contact with others in the education world. Electronic information-handling skills are now fundamental to the preparation of citizens and future employees. Staff are encouraged to investigate the possibilities provided by access to this electronic information and communication resource, and blend its use, as appropriate, within the curriculum. They should model appropriate and effective use, and provide guidance and instruction to pupils in the acceptable use of the Intranet/Internet.
• It is not permitted for staff to invite or accept pupils onto personal social networking sites – refer to Marlborough School's General Code of Conduct.
• Staff should be very sensitive to the content of any material they post on social networking sites given the audience. Some comments could be perceived as inappropriate or unprofessional. Such comments could lead to disciplinary action.
• Staff should be aware of Cornwall Council's Social Networking Guidelines.
• Cornwall LA supports the implementation and sharing of effective practices and collaborative networking across the LA as well as nationally and internationally. Please select appropriate websites to collaborate and ensure you are aware of the audiences.
• When using the internet, all users are expected to comply with all laws and government regulations concerning copyright, libel, fraud, discrimination and obscenity and all school staff are expected to communicate in a professional manner consistent with the rules of behaviour governing employees in the education sector.
• Pupils are responsible for their good behaviour on the school networks, just as they are on and off school premises. While the use of information and communication technologies is a required aspect of the National Curriculum, access to the Intranet/Internet is a privilege – not a right. It will be given to pupils who act in a considerate and responsible manner, and may be withdrawn if they fail to maintain acceptable standards of use.

Staff should ensure that pupils know and understand that, in addition to the points found under Online activities which are not permitted, no online user is permitted to:

• Retrieve, send, copy or display offensive messages or pictures.
• Use obscene or racist language.
• Harass, insult or attack others.
• Damage computers, computer peripherals, computer systems or computer networks.
• Violate copyright laws.
• Use another user's login account.
• Trespass in another user's folders, work or files.
• Use the network for commercial purposes.
• Use the network to promote extremism of any kind.

Supervising and Monitoring Usage

Teachers should guide pupils toward appropriate online materials. This will avoid a great deal of time wasting as well as going some way towards monitoring the sites accessed by pupils.

Online access for pupils should be available only on computers that are in highly used areas of the school such as classrooms and the library. Online machines should be in full view of people circulating in the area. Children should never use online services without supervision.

While using the internet at school, pupils should be supervised. However, when appropriate to their age and their focus of study, pupils may pursue electronic research independent of staff supervision; this should be at the discretion of the teacher in charge. Some children, particularly those on the Record of Need may require more supervision relative to their level of need and understanding. Network administrators may review files and communications to maintain system integrity and ensure that users are using the system responsibly. While normal privacy is respected and protected by password controls, as with the internet itself, users must not expect files stored on school servers to be private.

Appendix 1 Online Safety – examples of risks

- 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
- inappropriate communication / contact with others, including strangers
- radicalisation*
- the sharing / distribution of personal images without an individual's consent or knowledge
- cyber-bullying
- access to unsuitable video / internet games
- an inability to evaluate the quality, accuracy and relevance of information on the internet
- plagiarism and copyright infringement
- illegal downloading of music or video files
- the potential for excessive use of ICT which may impact on the social and emotional development and learning of the young person

*__Radicalisation__

nb Extremism the holding of extreme political or religious views.
Radicalisation the process by which an individual/groups come to adopt increasingly extreme political, social, or religious ideals and aspirations.

The school protects the right to freedom of expression but, whilst it has no policy or intention to restrict or prevent legitimate debate, does tackle any threat of extremism and or terrorism within our school community. This is the responsibility of the Designated Safeguarding Lead.

As is the school's responsibility under law, we will do our utmost to safeguard our pupils from being drawn into extremism and terrorism. The school has strong relationships with our Local Safeguarding Children Board (LSCB) and local police, and will not hesitate to involve them at the earliest opportunity if safeguarding issues arise.

Because visitors and speakers coming into the school are appropriately vetted prior to them having access to pupils, and materials handed out to pupils checked, this same level of care needs to apply to the use of the internet.

Children's use of computers and access to the World Wide Web is supervised and monitored. The school has an effective firewall and block on inappropriate sires through its internet provider via Croft Technologies.

Appendix 2 Online Safety – User Responsibilities

For the professional and personal safety of adults, the responsibilities set out in this document also apply to use of school IT systems (laptops, email, etc.) out of school and any personal equipment used in school.

Administrator/ IT Support

- oversees the provision of class user names and passwords
- ensures the admin and teaching staff passwords are kept securely in school safe
- maintains the records of details of the access rights
- records any actual or potential e-Safety incident as reported by all other users
- liaises with the headteacher concerning all e-Safety incidents
- maintains and alters the filter service
- logs any changes to the filter system
- reports any filtering issues to the service provider immediately
- maintains a record of all downloaded .exe files which have been agreed for staff use
- installs curriculum software on school workstations / portable devices
- liaises with ICT infrastructure support team to ensure appropriate safety systems and security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data
- liaises with ICT infrastructure support team to ensure appropriate virus software is maintained
- attends Online Safety training
- keeps staff informed of issues
- disseminates training where appropriate

Adults:

- have an individual user name and password;
- are responsible for the security of their username and password; must not allow other users to access the systems using their log on details; must immediately report any suspicion or evidence that there has been a breach of security
- must not access, copy, remove or otherwise alter any other user's files, without their express permission
- ensure that any personal hand held / external devices (laptops / mobile phones / USB devices etc) are protected by up-to-date anti-virus software; are free from viruses and password protected where possible
- ask permission of the IT technician and or headteacher before:
    - down/uploading large amounts of data which might prevent other users from being able to carry out their work e.g., photos, videos, .exe files and /or apps
    - installing or attempting to install programmes
    - altering or disabling computer settings
- ensure sensible and appropriate security measures such as encryption are in place to protect any sensitive data removed from the school site
- must not download or distribute copies of copyrighted material including music and videos
- must not engage in any on-line activity that may compromise professional responsibilities
- observe the school's understood protocol for the use of laptops, portable devices etc. used out of school with regard to:
    - the extent of personal use
    - access for family members

    - use of removable media e.g., memory sticks etc;
    - use of apps and other software
- regularly reinforce online safety messages in the use of IT across the curriculum
- pre-plan the use of the internet for children; pre-checking sites for suitability
- monitor vigilantly the content of the websites visited where pupils are allowed to freely search the internet
- teach children to:
    - be critically aware of the materials / content they access on-line
    - validate the accuracy of information
    - acknowledge the source of information used
    - respect copyright when using material accessed on the internet
- may request sites to be removed from the filtered list for specific purposes
- report any unsuitable material that is found in internet searches immediately to IT technician for filtering
- report any actual / potential online safety incident to IT technician
- ensure the safe use of digital and video images, as follows:
    - teach pupils about the risks associated in taking, using, sharing, publishing and distributing images; particularly recognising the risks attached to publishing their own images on the internet
    - use digital / video images to support educational aims only when following relevant school procedures regarding sharing, distributing and publishing of those images including checking parental permission document
    - ensure that no photographs are taken which bring individuals or the school into disrepute
    - ensure photographs published on the website, or elsewhere which include pupils are selected carefully and comply with good practice guidance on the use of such images
    - must not use pupils' full names on any website or blog, particularly in association with photographs
    - ensure all images adhere to the school's data protection policies

Appendix 3 Online Safety – Communications

We recognise that communications technologies can enhance learning. It can also appropriately support teachers' and pupils' personal needs; the table below outlines acceptable and desirable use.

Mobile Phones: The school understands that some pupils are issued with mobile phones for good reason. However, if a pupil is found to be using a mobile phone, it can be confiscated as a disciplinary penalty and school staff have a legal defence in respect of this in the Education and Inspections Act 2006 (S94). In order to protect all staff and pupils the following rules apply:
• Pupils with mobile phones should hand them in to the office first thing in the morning and collect them at the end of the school day.
• Staff should not usually use personal mobile phones to contact parents. If mobile devises are used staff are to either switch off caller I.D. or put 141 in front of the number called so their phone number is withheld from the recipient.
• Staff mobile phones should be kept on silent during the school day.
• Should a staff mobile phone go missing in school this should be reported to the Headteacher and the Police.
• Staff should never loan their personal mobile phones to pupils.

Email Communication- Adults

- should use the school email service by default
- use email with professional responsibility and appropriate tone
- need to be aware that email communications may be monitored
- must immediately report to the headteacher any inappropriate or concerning emails (without responding to such messages)

Email Communication - Pupils

- must use whole class or group email addresses
- must write clear and correct emails and not include any unsuitable or abusive material
- must follow all the email safety issues, such as the risks attached to the use of personal details about which they are taught
- must report any inappropriate emails to their teachers or a responsible adult
- must not post any personal information
- may only ever communicate with teachers by using either the class or teacher's school email address

	Adults	Children
Mobile phones May be brought to school May be used in lessons/playtime May be used in social time	 Yes No Yes	 Yes No No
Instant messaging	With headteacher's authorisation	With headteacher's authorisation
Personal email addresses	Yes	Yes, for Coding Club and Scratch
Personal use of school email	With headteacher's authorisation	No
Chatrooms	Yes, during social times or as appropriate	supervised curricula purposes
Social networking	Yes, during social times or as appropriate	supervised curricula purposes

Blogs	Yes, during social times or as appropriate	supervised curricula purposes

Appendix 4 Online Safety – Misuse Guide

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse: If any apparent or actual misuse appears to involve illegal activity, ie:

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the SWGfL "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress" should be followed. This can be found on the SWGfL Safe website within the "Safety and Security booklet". This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer.

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

Pupils

Incident	Actions / Sanctions
Deliberately accessing or trying to access illegal material	Refer to headteacher; inform parents; refer to police as appropriate
Unauthorised use of non-educational sites during lessons	Class teacher to manage using Marlborough Manners structure
Unauthorised use of mobile phone / digital camera / other handheld device/ Smart watch	Phones/ Smart watches not used in school
Unauthorised use of social networking / instant messaging / personal email	Refer to headteacher; inform parents
Unauthorised downloading or uploading of files	Refer to headteacher
Allowing others to access school network by sharing username and passwords	Refer to headteacher; inform parents
Attempting to access or accessing the school network, using the account of a member of staff	Refer to headteacher; inform parents
Corrupting or destroying the data of other users	Class teacher to manage using Marlborough Manners structure

	Refer to headteacher; inform parents
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	Class teacher to manage using Marlborough Manners structure; refer to headteacher; inform parents; refer to police as appropriate and as necessary
Continued infringements of the above, following previous warnings or sanctions	Refer to police as appropriate; where illegal inform parents and refer to police. All other cases consider school sanctions – seclusion, exclusion.
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	Class teacher to manage using Marlborough Manners structure
Using proxy sites or other means to subvert the school's filtering system	Refer to headteacher; inform parents
Accidentally accessing offensive or pornographic material and failing to report the incident	Refer to headteacher; inform parents
Deliberately accessing or trying to access offensive or pornographic material	Refer to headteacher; inform parents; refer to police as appropriate
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	Refer to headteacher

Staff

Incidents:	Actions / Sanctions
Deliberately accessing or trying to access illegal material	Refer to headteacher – oral warning/ written warning /suspension /disciplinary action; inform governors; refer to police as appropriate
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	Refer to headteacher – oral warning
Unauthorised downloading or uploading of files	Refer to headteacher – oral warning
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	Refer to headteacher – oral warning/ written warning /suspension /disciplinary action; inform governors
Careless use of personal data eg holding or transferring data in an insecure manner	Refer to headteacher – oral warning; potentially could be taken further
Deliberate actions to breach data protection or network security rules	Refer to headteacher – oral warning/ written warning /suspension /disciplinary action;

	inform governors
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	Refer to headteacher – oral warning/ written warning /suspension /disciplinary action; inform governors
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	Refer to headteacher – oral warning/ written warning /suspension /disciplinary action; inform governors
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils	Refer to headteacher – oral warning
Actions which could compromise the staff member's professional standing	Refer to headteacher – oral warning
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	Refer to headteacher – oral warning/ written warning /suspension /disciplinary action; inform governors
Using proxy sites or other means to subvert the school's filtering system	Refer to headteacher – oral warning/ written warning /suspension /disciplinary action; inform governors
Accidentally accessing offensive or pornographic material and failing to report the incident	Refer to headteacher – oral warning
Deliberately accessing or trying to access offensive or pornographic material	Refer to headteacher – oral warning/ written warning /suspension /disciplinary action; inform governors
Breaching copyright or licensing regulations	Refer to headteacher – oral warning/ written warning /suspension /disciplinary action; inform governors; refer to police as appropriate
Continued infringements of the above, following previous warnings or sanctions	Refer to headteacher – oral warning/ written warning /suspension /disciplinary action; inform governors; refer to police as appropriate