 <p>Offley Endowed Primary School & Nursery</p>	<h1>Offley Endowed Primary School and Nursery</h1>	<p>Reviewed: Mar 2026</p> <p>Next Review: Mar 2028</p>
<p>Policy Title:</p>	<h2>E Safety Policy</h2>	<p>Users: Staff, Governors, Parents</p>

Statement of Intent:

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, 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.

At Offley Endowed we recognise that new technologies can also present dangers to our children and that keeping them safe 'on line' is an important part of our safeguarding responsibilities. This policy and its appendices set out the principles and procedures underpinning our approach to e-safety including data protection. It should also be read in conjunction with all safeguarding policies and curriculum policies including ICT and PSHCE.

Definition of ICT:

ICT or Information Communication Technology includes but is not limited to the following:

- Websites
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality
- Gaming, especially online
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading

Infrastructure

All users of the schools computer network have clearly defined access rights enforced by using a user name and login system. Account privileges are achieved through the file/folder permissions, and are based on each user's requirements. Children have much more limitations in place than individual staff members do with their personal logins. This helps to protect the network from accidental or malicious attempts to threaten the security of it or the data accessible using it. Guests (e.g. supply teachers) are requested to login using a visitor login to prevent them viewing any potentially confidential data that might be stored on the school's drives.

A permanently-enabled filtering system (provided by Primary IT) is used, it is designed to filter out material found to be inappropriate for use in the education environment.

Access to make changes to overwrite the base-default setting to allow or deny access to a particular website URL can be achieved by contacting the ICT subject leader or school administrator. All changes

Approved and Adopted by Governing Body



Offley Endowed Primary School and Nursery

E Safety Policy

Reviewed: Mar 2026

Next Review: Mar 2028

made to internet filtering are logged by them to help prevent abuse of the system. Security software is installed on all Windows machines to prevent any malware attacks.

Guidelines:

Pupils Rules for Acceptable Use

- Pupils will ask permission from a member of staff before using devices.
- Pupils will use devices safely and appropriately.
- Pupils will not deliberately seek out inappropriate websites.
- Pupils will report any inappropriate material they may come across to a staff member immediately in order to help protect themselves and others.
- Pupils will not download or install any programs or files.
- Pupils will ask permission before completing and sending online forms.
- Pupils will not give out any personal information over the internet.
- Pupils will not share their log in details with others.
- Pupils will be polite and respectful when communicating with other people on the internet.
- Pupils understand that the school can and may monitor their internet usage and check the sites they visit and their files.
- Pupils will be encouraged to use strong passwords.
- A list of rules for using the internet safely will be displayed in all classrooms.

Staff and Governors Rules for Acceptable Use:

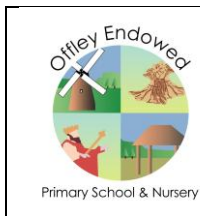
Staff and governors are contractually obliged to use the internet safely, appropriately and professionally within school following the same expectations and rules given to visitors. They are aware that they are role models for others and so should promote and model a high expectation of behaviour at all times.

Whilst checking of personal sites e.g. email is permitted outside of pupil contact time, it is recognised that this should only happen for brief periods of time and is merely a privilege and thus can be removed at any time.

Visitors Rules for Acceptable Use:

- Visitors will use the internet safely and appropriately.
- They will use the IT facilities with respect.
- They will not deliberately seek out inappropriate websites.
- They will report any unpleasant material to a staff member, in order to protect themselves and others.
- They will not download or install programs or files on the school network, to minimise the risk of viruses.
- They will not share the log in details.
- They will be polite and respectful over the internet.
- They will not use our internet for our own financial gain, political purposes or advertising personal or private business.
- They understand that the school can and may check files and monitor internet sites visited.

General



Offley Endowed Primary School and Nursery

E Safety Policy

Reviewed: Mar 2026

Next Review: Mar 2028

1. The governors appoint the Headteacher to oversee all operational aspects of e-safety.
2. There is a list of acceptable usage rules which are displayed in every classroom. (See Appendix A) A copy is sent to all families for parents to read and discuss with their children.
3. All staff, governors and volunteers are reminded of their professional responsibility in relation to e-safety on an annual basis. (See Appendix B)
4. The Headteacher will undertake an annual assessment of e-safety needs in relation to new technologies within the school and wider community.
5. The governors give relevant staff access to its Management Information System with a unique username and password. All data will be encrypted with passwords wherever possible.
6. Members of staff are required to ensure the security of any personal, sensitive, confidential or classified information. This includes laptops and memory sticks.
7. Members of staff are required to use school email accounts for school business. Where confidential or sensitive information is being transferred by email, express consent must be sought from the Headteacher and a password encryption must be in place.
8. Personal mobile phones are not to be used during lesson time and should never be used to take photographs of children.

Rules for Publishing Material Online (including Images of Pupils)

Whilst we wish the school's website and Twitter page to be a valuable tool for sharing information and promoting children's achievements with a global audience, we do recognise the potential for abuse that material published may attract, no matter how small this risk may be. Therefore, when considering material for publication on the website, the following principles should be kept in mind, in accordance with the school's Child Protection Policy:

- If an image/audio/video recording of a child is used then they should not be named (including in credits).
- If a pupil is named, their image/audio/video recording should not be used (no surnames should be published).
- Files should be appropriately named in accordance with these principles and care should be taken to include only suitable ALT tags as well.
- Only images of children in suitable dress should be used and group photographs are preferred in preference to individual photographs.
- Parents are given the opportunity to withdraw permission for the school to publish images/audio/video of their child on the school website.
- Content should not infringe the intellectual property rights of others – copyright may apply to: text, images, music or video that originate from other sources. All copied or embedded content should be properly referenced.
- Content should be polite and respect others.
- Material should be proof-read (e.g. to check for spelling or grammatical errors) before being published.
- Photography is permitted at all school events. Parents are reminded about safe use of images before the performance begins and are requested not to post images on social networking sites.

Comments submitted to posts on the website must be moderated by the post's author before being published (to ensure they are appropriate and reveal no personal information).



Offley Endowed Primary School and Nursery

E Safety Policy

Reviewed: Mar 2026

Next Review: Mar 2028

Children will likely use a variety of online tools for educational purposes during their time at the school. They will be asked to only use their first name or a suitable avatar for any work that will be publicly accessible and be required to follow the principles listed above before sending any work for publishing. Staff should encourage contributions that are worthwhile and develop a particular discussion topic.

When photo/videos of school events (e.g. plays) are permitted to be taken by watching parents for personal memories, they will be asked not to publish them onto any public area of the Internet, including social networking sites.

Social Media:

Staff and children are not permitted to access their social media accounts whilst at school. When accessing them outside of school hours they should be mindful of not bringing the profession or school into disrepute.

Breaches:

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. Policy breaches may also lead to criminal or civil proceedings.

Incident Reporting:

Any security breaches or attempted breaches, loss of equipment or any unauthorised use or suspected misuse of ICT must be immediately reported to the Headteacher or in the instance that the Headteacher is the suspect, the Chair of Governors.



Offley Endowed Primary School and Nursery

E Safety Policy

Reviewed: Mar 2026

Next Review: Mar 2028

Internet

Internet Use Contracts

Pupils and parents are asked to read, complete and sign an internet use contract which details expected behaviour when using the internet in school. These contracts will be given out annually to new pupils. Parents must consent to their child/ren using the internet in school.

Guidelines for appropriate use are as follows:

- Pupils will ask permission from a member of staff before using devices.
- Pupils will use devices safely and appropriately.
- Pupils will not deliberately seek out inappropriate websites.
- Pupils will report any inappropriate material they may come across to a staff member immediately in order to help protect themselves and others.
- Pupils will not download or install any programs or files.
- Pupils will ask permission before completing and sending online forms.
- Pupils will not give out any personal information over the internet.
- Pupils will not share their log in details with others.
- Pupils will be polite and respectful when communicating with other people on the internet.
- Pupils understand that the school can and may monitor their internet usage and check the sites they visit and their files.
- Pupils will be encouraged to use strong passwords.

E-safety Education and Training

E Safety in the Curriculum:

ICT and online resources are increasingly used across the curriculum. We believe it is essential for E Safety guidance to be given to the pupils on a regular and meaningful basis. E-Safety is embedded within our Computing and PHSE curriculum and we continually look for new opportunities to promote E-Safety. The following aspects are taught at each stage:

EYFS/ KS1

At this level, use of the Internet will either be quite heavily supervised or based around pre-selected, safe websites. Children will be regularly reminded about how to always take care when clicking and to seek help/advice from an adult if they see anything that makes them unhappy or that they are unsure about.

Lower KS2

Children will now be given more opportunities to develop their digital literacy skills. They will be shown how to develop a responsible attitude towards searching the World Wide Web and will be reminded of the need to report any concerns they have. The importance of creating strong passwords and the benefits of only joining child-friendly websites will also be taught.

Upper KS2

Children will now be encouraged to become more independent at researching for information on the World Wide Web, being taught the necessary skills to critically evaluate sites for accuracy and suitability. They will be supported in using online collaboration tools more for communicating and sharing ideas with others, including being taught the need for not revealing personal information to strangers. The aim



Offley Endowed Primary School and Nursery

E Safety Policy

Reviewed: Mar 2026

Next Review: Mar 2028

is to teach them how to manage and deal with risks they encounter by themselves, whilst at the same time encouraging them to become positive users of both new and emerging technologies.

E-safety for Staff, Governors and Parents

The school will provide regular e-safety training for staff, governors and parents. The school understands the need to keep children safe whilst they enjoy computing and are keen to share this with all parties. For these reasons the school provides an acceptable use policy, advise for parents on the use of social networking systems and regular e-safety update meetings.

Guidance for use of Social Networking Systems.

The school recognises that many staff and parents will actively use Facebook, Twitter and other social networking platforms; including to support their personal development and learning. Staff must recognise that it is not appropriate to discuss issues relating to children or other staff via these networks. Discretion and professional conduct are essential. Staff are encouraged to review their privacy settings and make sure their profiles and photographs are not viewable by the general public. It's never acceptable to accept a friendship request from a child, as in all cases children of primary age using such networks will be breaching the terms and conditions, it is also extremely inadvisable to accept friend requests from ex-pupils who are still minors, as this behaviour could be construed as grooming. Staff should not give out their personal details to pupils including home or mobile telephone numbers and personal emails. All correspondence should be through the school system.

Responding to Unacceptable Internet Use by:

Pupils:

Pupils should be made aware that all e-safety concerns will be dealt with promptly, sensitively and effectively so that they will feel able and safe to report any incidents.

Children are encouraged to respect the facilities offered to them, however, staff are trained in how to proceed following a breach of the rules for acceptable internet use, in accordance with the schools safe guarding policy. This includes guidance on preservation of evidence and immediate reporting. The school's child protection officer has overall responsibility for internet safety so any misuse should be reported to them without delay.

Depending on the severity and nature of the misuse offence, sanctions include: first warnings, temporary bans from using the ICT resources and meetings with parents and carers. All incidents should be recorded.

Staff, Governors and Visitors

Failure to comply with the rules for responsible internet use could lead to sanctions being imposed and possible disciplinary action being taken, in accordance with the schools safe guarding policy, child protection policy and the law. Misuse should be reported without delay.



Offley Endowed Primary School and Nursery

E Safety Policy

Reviewed: Mar 2026

Next Review: Mar 2028

Data Protection and Data Backup:

All data held on the school network is subject to the data protection act 1998. Unlicensed or personal software must not be installed on the system, if software is deemed to be of use to the school, it should be duly acquired under a school licence.

Where personal data such as school reports, IEP's, correspondence and assessment is taken home on a school lap top or other portable storage devices, it must be recognised that this data comes under the data protection act and therefore, every care must be taken to ensure its integrity and security. It should be removed from any portable device including USB pens and memory cards as soon as possible.

If using a USB pen or memory card it is the user's responsibility not to transfer any viruses onto the schools network. Pupils are prohibited from using such media.

Staff are encouraged to use the drives on the school network as a central place for documents such as policies and planning files. Confidential pupil data maybe safely stored here as it is accessible only through login by school staff.

All pupil work is stored in their own personal folder on the network. Children's files cannot be removed or deleted whilst logged onto a machine as a pupil user.

The servers containing these networked devices are locked away each night as an extra security measure to prevent theft.

Data stored on the schools networked drives is backed up regularly so copies of files may be recovered if the original becomes lost or damaged.

Home learning – (added due to partial school closure due to Coronavirus)

Rules for Remote Learning

- I understand that a Home learning lesson or contact through MS Teams will be subject to the same school rules which apply in face to face lessons.
- I will follow all instructions issued by my teacher, only using technology as they direct me to do.
- I will make sure my communication with teachers and other children is of the same formality expected in a normal classroom environment.
- I will be responsible for my behaviour and actions when using MS Teams
- I will not deliberately access or share any material which could be deemed illegal or offensive. If I come across such material I will report it to a suitable adult, either my teacher or parents.
- I will not contact my teachers outside the hours of 9am to 3:30pm.
- I will not request one to one sessions with my teachers via MS Teams or any other platform.
- I will not record or take photos of my teachers or classmates, or any lesson content



Offley Endowed Primary School and Nursery

E Safety Policy

Reviewed: Mar 2026

Next Review: Mar 2028

- I understand that these rules are designed to keep me safe and that if they are not followed the normal school behaviour policy will be invoked.
- Ensure you are in a quiet, safe and appropriate environment with minimal distractions. A bedroom is not likely to be a suitable location; a dining or kitchen table, if suitably quiet, may be appropriate.
- Log in promptly when you receive the invitation from your teacher.
- Dress appropriately. No pyjamas and fully clothed.
- Ensure you are attentive and follow all instructions, treating others with kindness and patience, particularly where technical issues cause disruption.
- If you are in a live MS Teams session, end your session when your teacher indicates it is complete.
- *You may not record lessons or any other online interactions. Your teachers will provide all the materials you need.*

Policy Review.

The policy is reviewed regularly to respond to any significant new developments in the use of technologies, new threats to e-safety and incidents that have taken place.