

The Federation of Llanfoist Fawr and Llanvihangel Crucorney Primary Schools



Online Safety Policy

Agreed January 2026 to be reviewed January 2030

Signed.....S Davies..... Headteacher

Signed.....M Davies..... Chair of Governors

ONLINE Safety POLICY

Online safety encompasses the use of new technologies, internet and electronic communications such as: mobile phones, collaboration tools and personal publishing.

The school's online safety policy will operate in conjunction with other policies including: Pupil Behaviour, Anti-Bullying, Child Protection, PSE Policy, Curriculum and MCC Safer Distance Learning Policy.

Online safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of online safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband including the effective management of filtering.
- A member of staff being responsible for the implementation and monitoring of this online safety policy.

INTRODUCTION

The purpose of this policy is to:

- Through consultation with pupils establish the ground rules we have in the Federation for using the Internet and electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.
- Describe how these fit into the wider context of our safeguarding, behaviour and RSE policies.
- Demonstrate the methods used to protect children from sites containing pornography, racist or politically extreme views and violence.
- Understand that accessing inappropriate sites accidentally is not something to feel guilty about and that any such incident should be reported to staff immediately.

TEACHING AND LEARNING

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- The school acknowledges the potential benefits of the use of gen AI in an educational context - including enhancing learning and teaching, improving administrative processes, managing workload and preparing staff and learners for a future in which AI technology will be an integral part. Staff and pupils are encouraged to use gen AI based tools to support their work where appropriate, within the frameworks provided below and are required to be professionally responsible and accountable for this area of their work.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school ensures that the use of Internet derived materials by staff and pupils complies with copyright law.

- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The ICT curriculum is driven by the DCF and is overarched by the AoLE Science and technology. Pupils are taught how to communicate respectfully, understand personal and private information and consider health and wellbeing aspects of using technology.

MANAGING INTERNET ACCESS

- School ICT systems capacity and security is reviewed regularly by the school and the Share Resource Service (SRS)
- Virus/ firewall protection is updated regularly by SRS.
- We will comply with all relevant legislation and guidance, with reference to guidance contained in Keeping Learners Safe.

E-mail

- Pupils may only use approved Hwb e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication or arrange to meet anyone.

School web site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information is not published.
- The head teacher has overall editorial responsibility and ensures that content is accurate and appropriate.
- Photographs that include pupils are selected carefully so they do not enable individual pupils to be clearly identified.
- Pupils' full names are not used anywhere on the Web site or blog.
- Written permission from parents or carers must be obtained before photographs of pupils are published on the school Web site (see Appendix 1 for sample permission form).
- Pupil's work will only be published with the permission of the pupil and parents.

Social networking and personal publishing

- SRS blocks access to social networking sites.
- Newsgroups are also blocked.
- Pupils are told never to give out personal details of any kind which may identify them.
- Pupils and parents are advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Managing filtering

- If staff or pupils discover an unsuitable site, it must be reported immediately to the e- Safety Coordinator who will reported to SRS for them to add to their filtering list.
- Senior staff ensures that regular checks are made to ensure that the filtering methods are appropriate and effective.

Managing emerging technologies

- Emerging technologies are examined for educational benefit and a risk assessment is carried out before use in school is allowed.
- Mobile phones are not used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

Managing the use of Artificial Intelligence

- As artificial intelligence (AI) tools become more common in school and at home, it is important that children learn to use them safely and responsibly. In the Federation, pupils are taught that AI systems—such as chatbots or apps that generate pictures or information—are tools, they are not people, and should always be used with adult supervision. Pupils learn never to share personal information with any online tool, including AI, and to check with a trusted adult if something they see or read feels confusing or upsetting. Staff help pupils understand that AI can sometimes make mistakes, so information found through these tools should be checked and discussed. By building these skills early, pupils learn to use new technologies confidently, thoughtfully, and safely.
- As set out in the staff acceptable use agreement, staff will be supported to engage with gen AI tools responsibly, ensuring the protection of both personal and sensitive data.
- Improper use of gen AI tools, including breaches of data protection standards, misuse of sensitive information, or failure to adhere to this agreement, will be subject to disciplinary action as defined in Staff Disciplinary Policy.

Protecting personal data

- Personal data is recorded, processed, transferred and made available according to the Data Protection Act 2018. The school meets all of its GDPR requirements.
- Staff will always ensure gen AI tools used comply with UK GDPR and other data protection regulations, verifying with the Data Protection Officer (DPO) that tools comply with standards set by the Information Commissioner's Office (ICO) before using them for work related to the school.

POLICY DECISIONS

Authorising Internet access

- All staff read and sign the 'Acceptable ICT Use Agreement' during induction before using any school ICT resource (see Appendix 2 for sample Staff Agreement).
- The school keeps a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance if a member of staff leaves or a pupil's access is withdrawn.
- In the Lower Phase, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- At Upper Phase, access to the Internet will be by supervised access to specific, approved online materials.

Assessing risks

- The school takes all reasonable precautions to ensure that user's access only appropriate material by using SRS filtering system.
- The school audits ICT provision on an annual basis to establish if the online safety policy is adequate and that its implementation is effective.

Handling online safety complaints

- Complaints of Internet misuse are dealt with by a senior member of staff.
- Any complaint about staff misuse is referred to the head teacher.
- Complaints of a child protection nature are dealt with in accordance with the school's child protection procedures.
- Pupils and parents are informed of the complaints procedure.

COMMUNICATIONS

Introducing the online safety policy to pupils

- Online safety rules are posted in all networked rooms and discussed with the pupils at the start of each year (see Appendix 3 for Internet Safety Rules).
- Pupils are informed that network and Internet use will be monitored.
- As part of the National Curriculum and skills development, all pupils are taught elements of the DCF which includes how to use ICT equipment safely and strategies to seek help of the child exploitation and online protection centres e.g. www.thinkuknow.co.uk

Staff and the online safety policy

- All staff have copies of the school's Online Safety Policy and know its importance.
- Staff are aware that Internet traffic can be monitored and traced to the individual user.
- Staff should always use school-provided accounts for work purposes. These accounts are configured to comply with organisational security and oversight requirements, reducing the risk of data breaches.

Enlisting parents' support

- Parents' attention is drawn to the school's Online Safety Policy in newsletters, the school brochure and on the school Web site.

This policy will be reviewed on an annual process by the governors and staff or in light of new guidance.

Appendix 1 - Lower Phase

Think then Click

These rules help us to stay safe on the Internet



We only use the internet when an adult is with us

We can click on the buttons or links when we know what they do.



We can search the Internet with an adult.

We always ask if we get lost on the Internet.



We can send and open emails together.

We can write polite and friendly emails to people that we know.



Think then Click

Online Safety Rules for Upper Phase

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we not sure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.
- We do not use Internet chat rooms.

Appendix 2

The Federation of Llanfoist Fawr and Llanvihangel Crucorney Primary School Staff Acceptable Use Policy for ICT

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's online safety policy for further information and clarification

- I understand that it could be deemed a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones; watches; digital cameras; e mail and social networking and that only ICT only authority owned (School) equipment should be used for school business.
- I understand that school information systems may not be used for private purposes without specific permission from the Head Teacher.
- I understand that my use of school information systems, internet and e mail may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone.
- I will not install any software or hardware without permission from the Head Teacher.

- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property right and adhere to the Data Protection Act 2018.
- I will report any incidents of concern regarding children's safety to the IT co-ordinator, the Designated Child Protection Co-ordinator or Head Teacher.
- I will ensure that electronic communications with pupils including email, instant messaging and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote online safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

The school may exercise its right to monitor the use of the school's information systems and internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Breach of the policy will be considered a serious disciplinary matter and will be dealt with in line with the Disciplinary Policy and procedure.

I have read, understood and accept the Staff Acceptable Use Policy for ICT/ social media.

Signed: Print Name: Date:

Appendix 3 – To be displayed in class

Lower Phase

These rules help us to stay
safe on the Internet

Think then Click



We only use the Internet when an adult is with us.



We can click on the buttons or links when we know what they do.



We can search the Internet with an adult.

Think then Click



We ask permission before using the Internet.

We only use websites our teacher has chosen.



We immediately close any webpage we don't like.

We only e-mail people our teacher has approved.



We send e-mails that are polite and friendly.

We never give out a home address or phone number.



We never arrange to meet anyone we don't know.

We never open e-mails sent by anyone we don't know.



We never use Internet chat rooms.

We tell the teacher if we see anything we are unhappy with.

