

ICT ACCEPTABLE USE POLICY

New technologies have become integral to the lives of children in today's society, both within school and in their lives outside school. The internet and other digital information and communication tools can stimulate discussion and promote creativity helping towards effective learning.

This policy applies to the school as a whole, including the Early Years Department.

This policy is intended to ensure:

- that children and adults will be responsible users and stay safe whilst using the internet and other communication technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

Fletewood School will try to ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect the pupils to agree to be responsible users. In line with the latest Keeping Children Safe in Education, the school has appropriate filtering and monitoring systems in place (see the Child Protection and Safeguarding policy).

Pupils' use of internet

Use of the internet, including e-mail, is permitted as directed by the teacher for purposes such as: - research and learning activities directly related to the curriculum.

Pupils will only be able to download a file under the direct supervision of a member of staff.

The use of game-style activities should be monitored by the teacher to determine suitability. Violent games are NOT permitted.

Personal e-mail, social networking or instant messaging sites are NOT to be accessed by pupils.

Children should report any misuse of the internet to their teacher.

Children should be made aware of the possibility and consequences of online bullying.

When e-mail is required as part of a curriculum-based lesson, ALL e-mails transmitted and received will be approved by teaching staff.

No e-mails will be approved where it may include information that may offend others or where it does not respect the rights, beliefs and feelings of others. Pupils of Fletewood School should always remember that they are representing themselves and our school.

Personal information such as full names, home addresses, and phone numbers will NEVER be sent by email.

Staff use of internet

- Use of the internet on school premises should principally be for school use, e.g. accessing learning resources, educational websites, researching curriculum topics, use of email on school business.

Use of the school's internet for personal financial gain (including the use of online auction sites), gambling, political purposes or advertising is prohibited.

Teachers should not be accessing the internet for personal reasons whilst teaching children.

Use of the internet to access any illegal sites or inappropriate material is a disciplinary offence. (If accessed accidentally users should report incident immediately to the Headteacher and it should be logged.)

The school recognises that many staff will actively use Facebook, Instagram, and other such social networking sites, blogging and messaging services. Staff must not post material (including text or images) which damages the reputation of the school or which causes concern about their suitability to work with children. Staff must recognise that it is not appropriate to discuss issues relating to children or other staff via these networks. Those who post material that could be considered as inappropriate could render themselves vulnerable to criticism or allegations of misconduct.

It is never acceptable to accept a 'friendship request' from pupils at the school, as in almost all cases children of primary age using such networks will be breaching terms and conditions of use of those networks. It is also extremely inadvisable to accept as friends, ex- pupils who are still minors. If a parent of a pupil seeks to establish contact, the member of staff should exercise their professional judgment, although it is recommended that contact is prohibited.

Setting a high security level on social networking sites is advisable.

Use of portable computer systems, USB sticks or any other removable media

- All sensitive data, such as children's details and reports, should be stored on an encrypted storage device or password-protected laptop. Other data, such as lesson plans and resources, may be stored on unencrypted devices.

Use of mobile phones

Staff should NOT use their personal phones for school business or for taking photographs of children, unless, in exceptional circumstances, an emergency telephone call needs to be made. It is to be noted that the school owns a mobile phone that should be taken on all school trips to be used for emergency contact.

Staff are allowed to bring their personal phones to school for their own use but will limit such use to non-contact time when pupils are not present and only use them in designated mobile phone areas. Staff members' personal phones will remain in either the school office or Class 1R stock cupboard during contact time with pupils. In

exceptional circumstances, such as childcare or medical emergencies, staff will be permitted to answer or make personal phone calls but only in designated mobile phone areas (school office, ministers' vestry).

Visitors and volunteers are not permitted to use their phones when on the school premises and must keep them in the school office.

Pupils should NOT bring mobile phones to school without the permission of the Headteacher. Permission is to be requested by the parent or guardian and reasons for the request must be stated. A request for permission does not imply that permission will be granted. All mobile phones will be collected by a staff member for safe keeping in the school office at the start of each school day and may be collected at the end of the day when the pupil leaves.

In order to protect both staff and parents, personal contact details should not be shared. If a staff member needs to contact a parent, they should do so via their official school email or via one of the school's phones. Should a parent need to contact a teacher, they should send an email to the staff member's/admin school email address or phone one of the school phones. Staff are only expected to respond to any such communications within term time working hours and cannot guarantee they will receive messages immediately. Working hours for teaching staff are between 8:30am and 4:30pm. The Headteacher can be contacted between 8am and 5pm. If a message is received outside of these times, it may not be replied to until the next working day.

Use of digital images

Following a review of our safeguarding procedures, and in line with the principles of Keeping Children Safe in Education (KCSIE) 2026, Fletewood School has made the decision not to publish identifiable images of pupils on public social media platforms and not to publish pupils' full names in any public-facing posts.

The digital landscape has changed significantly. Advances in artificial intelligence (AI) mean that photographs shared online can be copied, manipulated and misused in ways that were previously unimaginable.

National safeguarding organisations, the UK Safer Internet Centre, the National Crime Agency and the Department for Education have all highlighted the increasing risks associated with publicly available images of children, including AI-generated abuse material, identity misuse, grooming and online exploitation.

Whilst we are immensely proud of our pupils' achievements and enjoy celebrating their successes, we believe this can be done without compromising their privacy or digital safety.

Our commitment is to:

- Never publish a pupil's full name alongside any public image
- Avoid sharing identifiable photographs of pupils on public social media accounts
- Protect every child's digital identity and privacy

- Ensure all decisions relating to pupil images are guided by safeguarding, data protection legislation and the best interests of the child.

We will continue to celebrate learning, achievements and school life through photographs of activities, displays, performances, facilities and other non-identifiable content, that showcases our school community without placing our pupils at unnecessary risk.

Safeguarding is everyone's responsibility, and in an increasingly digital world, protecting a child's online identity is an essential part of keeping them safe.

The use of personal mobile phone cameras and/or cameras in the school is strictly prohibited. Where photographs are required, they must be taken on school cameras/phones/iPads and stored on a password protected device until no longer needed, whereby they should be deleted. Where possible, the use of the Tapestry app to upload photos is advised as all photos taken in this manner are stored solely on the secure Tapestry website and not on the device itself.

Ring Doorbells

Ring Doorbells have been installed at both main entrances to the school. This enables staff to see who is at the door before allowing entry. Images are recorded and streamed to the two school mobiles. Images stored from the previous day (or during school holidays) will be deleted at the start of the following day (or start of the new term). Only images that show suspicious activity will be kept for the purpose of evidence, should it be deemed necessary by the Headteacher.

Screen time in Early Years

Please see our Early Years and Foundation Stage policy for specific details on the use of screen time in Early Years.

Date last reviewed: September 2026

Next review date: September 2029