



Acceptable Use Policy

Policy Reviewed by:	Suzy Hollett (HR Manager)
Date:	01.08.2026
Policy Verified by:	Sara Llewellyn (School Leader-CEO)
Date:	08.08.2026
Date for Next Review:	01.09.2027

Legislation and Guidance

This policy should be read alongside:

- Keeping Children Safe in Education (KCSIE) September 2026
- Working Together to Safeguard Children 2026
- Data Protection Act 2018
- UK GDPR
- Education Act 2002 (Safeguarding Duties)
- Human Rights Act 1998
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Prevent Duty Guidance (current version)
- School's Online Safety Policy
- The School's Safeguarding and Child Protection Policy

ICT Resources

This policy aims to set guidelines and rules on the use of school ICT resources for our staff, pupils, school governors and visitors to the school. This Acceptable use policy should be read in relation to the school's Online Safety Policy and Safeguarding Policy and relates to other policies including Anti-Bullying and the school's complaints procedures.

The purpose of Internet access in schools is to raise educational standards, to support the professional work of staff and to enhance the school's management information and business administration systems. However, using ICT resources and facilities also poses risks to data protection, online safety and safeguarding so it is important that there are clear expectations in how staff and pupils engage with technology.

Access to the Internet and use of technology such as cameras are necessary tools for staff and an entitlement for pupil's who show a responsible and mature approach. It is our aim to have a clear policy on the acceptable use of mobile phones, ICT resources and equipment such as cameras that is understood and adhered to by all parties concerned without exception.

- The computer system is owned by the school and may be used by pupils to further their education and by staff to enhance their professional activities including teaching, research, administration, and management.
- The school's Internet Acceptable use policy has been drawn up to protect all parties - the pupils, the staff, and the school.
- All Internet activity should be appropriate to staff professional activity or the pupil's education.
- Personal details should remain private and should not be made available to other using the Internet.
- Access should only be made via the authorised account and password, which should not be made available to any other person.
- Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems is forbidden.
- Users are responsible for all E-mails sent and for contacts made that may result in E-mail being received.
- Use for personal financial gain, gambling, political purposes, or advertising is forbidden.
- Copyright of materials must be respected.
- Posting anonymous messages and forwarding chain letters is forbidden.
- As E-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.
- Use of the network to access inappropriate materials such as pornographic, racist, or offensive material is forbidden.

Mobile Phones

Maple Haven School allows staff to bring in personal mobile telephones and devices into the school, however, these are kept in staff lockers, unless prior arrangement is made with a member of the SLT or School leader for personal reasons. Each classroom has

their own mobile phone. Smart watches, tablets and other internet-enabled personal devices are subject to the same restrictions as mobile phones.

- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- All staff must ensure that their mobile telephones/devices are left on silent or switched off and left with their personal belongings throughout contact time with pupils.
- Mobile phone calls may only be taken at staff breaks or in staff members' own time.
- The phone numbers of each class mobiles and the reception phone and mobile should be given to all people likely to need a staff member during school time.
- If any staff member has a family emergency or similar and required to keep their mobile phone to hand, prior permission must be sought from the School Leader, Deputy Manager or Business Manager.
- It is the responsibility of all members of staff to be vigilant and report any concerns to the school Leader.
- Concerns will be taken seriously, logged, and investigated appropriately.
- Should inappropriate material be found then our Local Authority Designated Officer (LADO) will be contacted immediately. We will follow the guidance of the LADO as to the appropriate measures for the staff member's disciplinary action.

Photographs

- Photographs taken for the purpose of recording a pupil or group of pupils participating in activities or celebrating their successes should be only taken on the school mobile provided for the purpose.
- It is essential that photographs are taken and stored appropriately to safeguard the pupils in our care.
- Images taken on this mobile must be deemed suitable without putting the pupil in any compromising positions that could cause embarrassment or distress. All staff are responsible for the security of the mobile.

- Images taken and stored on the mobile must be downloaded as soon as possible and then deleted off the mobile device.
- Images will only be retained for as long as necessary and stored in accordance with the School's Data Protection Policy and Record Retention Schedule.
- Personal mobile phones must never be used to photograph or record pupils.

AI Use

Staff and pupils must only use artificial intelligence (AI) tools that have been approved by the School. AI-generated content must be reviewed for accuracy, safeguarding concerns, bias and data protection compliance before use.

Social Media

- Staff must maintain professional boundaries online.
- Staff must not accept friend requests from pupils.
- Staff must not communicate with pupils via personal social media accounts.
- Staff must not publish information, images or comments that may identify pupils without appropriate authority.
- Concerns arising from social media use must be reported to the DSL.

Cyber Security

Users must:

- Use strong passwords.
- Keep passwords confidential.
- Log out when devices are unattended.
- Report suspected phishing emails immediately.
- Report data breaches or cyber security incidents promptly.
- Not install software without authorisation.

Filtering and Monitoring

The School uses filtering and monitoring systems to safeguard pupils and protect ICT infrastructure.

Users should be aware that:

- Activity on school systems may be monitored.
- Internet activity may be logged.
- Concerns identified through monitoring may be investigated.

Failure to comply with these rules will result in one or more of the following:

- (a) Appropriate sanctions and restrictions placed on access to school facilities to be decided by the school Leader in accordance with the school's disciplinary procedures.
- (b) Any other action deemed appropriate under the School's Disciplinary Policy and Procedures.