POCKLINGTON CE (VC) INFANT SCHOOL
Acceptable Usage Policy

Date Reviewed:	January 2024
Date Due for Review:	July 2025
Contact Officer:	Tom Babington
Approved By:	Governors

Introduction and Aims;

Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for pupils, staff, governors, volunteers and visitors. It supports teaching and learning, and the pastoral and administrative functions of the school. However, the ICT resources and facilities our school uses could also pose risks to data protection, online safety and safeguarding. In order to keep the school community, including staff and children safe whilst working online we have developed this policy. This policy also needs to be read in conjunction with the following Pocklington CE Infant School policies: Acceptable Use, Child Protection, Safeguarding, Computing, Personal Development, Behaviour Policy and Statement of Behaviour Principles, Data Protection, Mobile Phone and Social Media as well as the East Riding of Yorkshire Council policies and guidance for Use of the Internet and Use of Electronic mail (Email). This policy reflects the school's aims and sets out what the school considers as 'Acceptable Use' of the ICT resources for all users of our computer network. It sets out a framework within which teaching and non-teaching staff can operate. It must be noted, however, that the school cannot guarantee complete safety from inappropriate materials.

Our aims for acceptable use at Pocklington CE Infant School are that:

- All stakeholders have a clear set of rules and guidelines on the use of school ICT resources including online interactions with one another.
- Disruption through misuse or attempted misuse of ICT resources is prevented.
- Teaching and learning of online safety and effective internet use is supported.

Acceptable Use Statement;

All members of the school community (staff including governors and volunteers) are required to read this policy. Staff and governors must sign the Acceptable Use Statement (Appendix 1). Parents/Carers/Guardians receive information on our AUP before their child starts at the school as part of the welcome pack.

If volunteers/visitors are required to use our computer network, they will also need to read this policy and sign the Acceptable Use Statement (Appendix 1). When visitors are attending a course/meeting on the school grounds which requires the use of the school devices/network, the course leader will read the Acceptable Use policy and sign the Acceptable Use Statement on behalf of all attendees and ensure the information within it is disseminated and adhered to.

We periodically check that all members of our school community have complied with this. These documents have been drawn up to protect anyone using the internet and our computer network. These documents have been reviewed and revised regularly.

Unacceptable use;

The following is considered unacceptable use of the school's ICT facilities. Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident. Unacceptable use of the school's ICTfacilities includes using the school's ICT facilities to:

- breach intellectual property rights or copyright
- bully or harass someone else, or to promote unlawful discrimination
- engage in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way
- access any illegal conduct, or statements which are deemed to be advocating illegal activity
- participate in online gambling, inappropriate advertising, phishing and/or financial scams
- access, create, store or create links to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- share consensual or non-consensual nude/semi-nude images and/or videos/livestreams
- undertake activity which defames or disparages the school, or risks bringing the school into disrepute including using inappropriate or offensive language
- share confidential information about the school, its pupils, or other members of the school community
- gain, or attempt to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- promote a private business, unless that business is directly related to the school
- use websites or mechanisms to bypass the school's filtering or monitoring mechanisms
- set up software, applications or web services on the school's network without

- approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the school's ICT facilities, accounts or data
- allow, encourage or enable others to gain (or attempt to gain) unauthorised access to the school's network
- cause a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation

Other forms of unacceptable use includes:

- breaching the school's policies or procedures
- connecting any device to the school's ICT network without approval from authorised personnel
- causing intentional damage to the school's ICT facilities
- removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel

Users;

a. Staff use

Access to school ICT

Staff will be provided with unique logins and passwords that they must use when accessing the school's ICT facilities. Staff must not access or attempt to access the school's ICT facilities using another member of staff's login details. If staff need their access permissions updated or changed, they must contact the school business manager.

Rules for Staff Device Use:

- Always transport devices in a protective case/bag
- Maintain the integrity of the device by treating it with care
- Do not leave devices in unsupervised areas, for example, vehicles or unlocked rooms (outside of school grounds)
- Do not leave the device unlocked when it is unattended in school
- Devices may be used for limited personal use subject to the restrictions contained in the Acceptable Use policy
- Devices must not be used by non-school employees.

Use of email

The school provides members of staff with an email address dependent upon their role. This email account should be used for work purposes only and all work-related business should be conducted using this account. Staff must not use the email address to sign up to mailing lists or newsletters unless they are work related, use the email address as a primary address for making personal purchases of goods and services from the internet linked to sites including but not limited to Amazon and eBay or to pay for goods by linking the account to applications such as Paypal.

Staff can share this email address with parents, but they must not share their personal email addresses with parents or pupils, and must not send any work-related materials using their personal email account. Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable. Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient. Emails sent by staff should not contain children's names and instead make use of their initials to identify them to other professionals where necessary. Staff should, instead, make use of the shared Google Workspace to share documents which contain children's names.

If staff receive an email in error, they should inform the school's Data Protection Officer immediately. If staff send an email in error that contains the personal information of another person, they must inform the school's Data Protection Officer immediately and follow the data breach procedure.

Use of phones

Staff must not give their personal phone number(s) to parents (unless approved by the headteacher) or pupils. Staff must use phones provided by the school to conduct all work-related business. School phones must not be used for personal matters unless authorised by a member of the senior leadership team.

Personal use of ICT facilities and materials

Staff are permitted to use school ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The headteacher may withdraw or restrict this permission at any time and at their discretion.

Personal use is permitted provided that such use:

- does not take place during teaching time
- does not constitute 'unacceptable use', as defined in section 3 of this policy
- takes place when no pupils are present
- does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes
- does not include using ICT facilities to store personal, non-work-related information or materials (such as music, videos or photos)

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities. Where breaches of this policy are found, disciplinary action may be taken. Staff should be aware that personal use of ICT can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents could see them.

Personal social media accounts

The term 'social media' is given to websites and online applications which allow users to interact with each other in some way – by sharing information, opinions, knowledge and interests. Examples include Facebook, Twitter, Snapchat, Instagram etc. Staff should make sure their use of social media, either for work or personal purposes, is appropriate at all times. Staff are responsible for any content they publish and must not publish content relating to Pocklington CE Infant School / East Riding of Yorkshire Council. Staff should take care to follow the school's guidelines on use of social media policy to protect themselves online and avoid compromising their professional integrity.

Pupil use

Access to ICT facilities and materials

Computers (including iPads) and other ICT resources are available to pupils only under the supervision of staff.

Personal Use

Children are not permitted to use school ICT facilities for personal use. Children who do not have an Acceptable Internet Use Statement agreed to on their behalf by their parent/carer/guardian will not be allowed to access the Internet. This will mean that pupils will not be able to use the devices stated above and will not be able to access all statutory content of the computing curriculum. Where a pupil does not have an agreed Acceptable Internet Use Statement in place, the parent/guardian/carer of the child will be contacted by the Computing Subject Leader to discuss the reasons why permission has not been granted and seek to find a solution.

Visitors, volunteers and members of the community

Visitors, volunteers and members of the community do not have access to the school's ICT facilities as a matter of course. However, those working for, or with, the school in an official capacity (for instance, as a volunteer, supply staff or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the school's facilities at the headteacher's discretion. When granted access in this way, they must abide by this policy as it applies to staff and sign an Acceptable Use Statement.

Parents

Parents are advised:

- Not to post images (including photos and videos) of pupils other than their own children on social media, unless they have the permission from parents of other children pictured.
- To raise queries, concerns or complaints directly with a member of staff, rather than posting on social media whether on their own pages, enclosed groups (e.g. groups set up for school parents to communicate with each other).
- Not to post malicious or fictitious comments on social media sites about any member of the school community.
- Not accessing social media on devices whilst supporting the school whether on site or on a school trip.

Monitoring and filtering of the school network and use of ICT facilities

To safeguard and promote the welfare of children and staff and provide them with a safe environment to learn, the school reserves the right to filter and monitor the use of its ICT facilities and network. Pocklington CE Infant School use a filtered internet service provided Securly. This includes, but is not limited to, the filtering and monitoring of: internet sites visited, bandwidth usage, email accounts, user activity/access logs, any other electronic communications. The effectiveness of any filtering and monitoring will be regularly reviewed. Where appropriate, authorised personnel may raise concerns about monitored activity with the Headteacher/DSL/Computing Subject Leader as appropriate. The school monitors ICT use in order to: Obtain information related to school business,investigate compliance with school policies, procedures and standards, ensure effective school and ICT operation, conduct training or quality control exercises, prevent or detect crime, comply with a subject access request, Freedom of Information Act request, or any other legal obligation. The governing board will regularly review the effectiveness of the school's monitoring and filtering systems.

GDPR 2018

Pocklington CE Infant School share personal data (e.g. name, date of birth) with third-party companies for the use of specific software packages, e.g. Scholar Pack. In order to comply with GDPR 2018, authorisation is required to process personal data in this way. Pocklington CE Infant School seek assurance from all third-party companies of their compliance with GDPR; this is done through the collation of their privacy notices. We have established records of processing activity which restrict the flow of data through the organisation and monitor against any risks associated with the processing of personal data.