Acceptable Use Agreement 2023/2024

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. This agreement is designed to ensure that all members of staff are aware of their professional responsibilities when using any form of technology.

Technology relates to ICT systems, hardware, software, internet, email, Learning Platforms, web2 technologies, mobile devices, cameras, laptops and memory devices.

Our aims for acceptable use at Settrington All Saints' Primary 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

Staff (including governors) are required to read this policy. Staff and governors must record that they have read the Acceptable Use Policy on GVO.

Pupils are taught about Acceptable Use and required to sign the ICT Acceptable Use Policy for Children on entry to the school and annually thereafter. A copy is kept on file.

Volunteers, visitors, 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 or student teacher) 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 the Student & Volunteers Induction document which identifies that they have read the policy..

Parents have access to this policy via the school website.

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 ICT facilities 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

Acceptable Use

The school business manager manages access to the school's ICT facilities and materials for all school staff. That includes, but is not limited to: computers, tablets, mobile phones and other devices as well as access permissions for certain programmes or files.

Members of staff:

• Must only use the school's technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body. It is a criminal offence to use an ICT system for uses other than those permitted by its owner.

• Must only use approved, secure school email systems for any school business.

• Must not browse, download or send material that could be considered offensive, and should report any accidental access of inappropriate materials to their line manager.

• Have a duty to protect their passwords and personal network and Learning Platform logins and should log off the network and Learning Platform when leaving a workstation unattended. Any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.

• Must not leave devices unlocked when unattended in school.

• Must not leave devices in unsupervised area, for example vehicles or unlocked rooms outside of school grounds, or allow use of devices by non-school employees

• Must not install any software or hardware without permission from a technician or the ICT coordinator.

• Are not permitted to use personal portable media for storage of school related data/images (e.g. USB stick) without the express permission of the Headteacher.

• Should ensure that personal data (such as data held on Scholarpack) is kept secure and is used appropriately, whether in school, taken off school premises, or accessed remotely. Personal data can only be taken out of school when authorised by the Headteacher or Governing Body.

• Are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, including when on external trips/visits. With the written consent of parents (on behalf of parents) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment. Digital images are easy to capture, reproduce and publish and, therefore, misused.

• Should ensure that their use of web 2 technologies, including social networking sites, such as Facebook, Twitter, META, TikTok, Instagram, YouTube and Myspace, does not question or bring their professional role into disrepute.

Members of staff:
- Are advised to consider, and set appropriately, their privacy settings on such sites.
- Should consider the appropriateness of images and material posted. Once posted online, a message, photo or video clip can be freely copied, manipulated and circulated and will potentially exist forever.

- Should not communicate with pupils, in relation to either school or non-school business, via web 2 technologies. Members of staff should only communicate with pupils using the appropriate LA/Academy learning platforms or other systems approved by the Headteacher.

• Are not permitted to contact or communicate with pupils, parents or conduct school business using personal email addresses or telephones, without specific permission from the Headteacher.

• Should not give out their own personal details, such as telephone/mobile number or email address, to pupils.

• Must ensure that all electronic communication with pupils and staff is compatible with their professional role.

• Must promote and model positive use of current and new technologies and e-safety. Members of staff can access information about e-safety from the North Yorkshire Primary ICT room and within the North Yorkshire Learning Platform and from the Learning Network. The e-safety coordinator can also provide information, resources and guidance.

• Must respect and comply with copyright and intellectual property rights.

• Have a responsibility to report any misuses of technology, including the unacceptable conduct of others, to the Headteacher. User Signature I agree to follow this user agreement and understand that failure to do so may result in disciplinary proceedings in the line with the School's Disciplinary Procedure.

Use of email

The school provides each member of staff with an email address. 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, or 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 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 online workspace to share documents which contain children's names.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information. 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.

Pupil use

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

Children are not permitted to use school ICT facilities without adult supervision and will be given direction to specific websites only as provided by the school.

Children are not permitted to use school ICT facilities for personal use.

Children will follow statutory content of the computing curriculum.

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. Settrington All Saints' Primary School use a filtered internet service provided by Schools ICT. 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. Only authorised personnel have access to this and may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law. The effectiveness of any filtering and monitoring will be regularly reviewed. Where appropriate, authorised personnel may raise concerns about monitored activity with the Online Safety Lead 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

Settrington Primary School share personal data (e.g. name, date of birth) with third-party companies for the use of specific software packages, e.g. Times Table Rockstars. In order to comply with GDPR 2018, authorisation is required to process personal data in this way. Settrington Primary 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.

Policy Review

This policy is reviewed and updated regularly to meet the changing needs of the school and in light of any new initiatives. The last review took place in **September 2023.**

Signature……M.Palmer…… Date……01/09/2023…….

Full Name (Printed)……M.Palmer……. Job title……Headteacher…….