ICT POLICY – ACCEPTABLE USE AGREEMENT (STAFF AND VOLUNTEERS)

Approval Date	October 2024
Policy Owner	Director of Operations
Adopted by Trust Board	Ratified by the Trust Board November 2024
Review Date	October 2026

CONTENTS

1. INTRODUCTION

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion and promote creativity, promoting effective learning. They also bring opportunities for staff to be more creative and productive in their work.

2. ACCEPTABLE USE POLICY

This Acceptable Use Policy is intended to ensure:

- That staff and volunteers will be safe and responsible users of the internet and other digital technologies.
- That school ICT systems and users are protected from accidental or deliberate misuse.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work and improve opportunities for learners and will, in return, expect staff and volunteers to agree to be responsible users.

3. ACCEPTABLE USE POLICY AGREEMENT

I understand that I must use school ICT systems in a responsible way, to minimise the risk to my safety or to the safety and security of the ICT systems and other users. I will, where possible, educate the young people in my care in the safe use of ICT and embed e- safety in my work with young people.

4. PROFESSIONAL AND PERSONAL SAFETY

For my professional and personal safety:

- I understand that the school will monitor my use of its ICT systems including email and other digital communications technologies. This may include but not be limited to the following circumstances:
    - With software to monitor 'trigger' words or phrases for safeguarding and to ensure acceptable, professional use of IT.
    - When staff leave or are on long-term absence for retrieval or redirection of messages.
    - When a member of staff is under investigation or suspected of illegal, fraudulent, inappropriate or safeguarding activity.
    - To collect and review information contained in any electronic system for documented purposes and authorised by **Head of IT & Infrastructure or Head of People**, for example, to complete a Subject Access Request or similar.
- I understand that information and resources stored on the organisations equipment and drives should be considered to be controlled and accessible by the school and authorised staff.
- I understand that this agreement also applies to use of school ICT systems out of school (e.g. laptops, email, VLE etc.). This includes my personal or work mobile phone or tablet if it contains my work email.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will keep my usernames and passwords private and will not try to use anyone else's username and password.
- I will not share or continue to use any logins for any school service or platform when I leave my employment.

- I will not attempt to circumvent technical controls on data storage and sharing, including any required control on personal devices to allow access to and management of School data.
- I will return all school owned ICT equipment and delete all school data from my personal devices when I leave my employment.
- I will immediately report any illegal, inappropriate or harmful material or incident, to the Head Teacher or other person appointed by the Head Teacher/DPO

5. PROFESSIONAL COMMUNICATION

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, delete or otherwise alter any other user's files, without their permission.
- I will communicate with others in a professional manner.
- I will ensure that when I take or publish images of pupils or parents/colleagues, I will do so with their permission and in accordance with the school's policy. I will not use my personal equipment to record these images, unless I have permission to do so.
- Where these images are published (e.g. on the school website / VLE) it will not be possible to identify pupils by name, or other personal information.
- I will not use chat and social networking sites in school.
- I will only communicate with pupils and parents / carers using official school systems and in a professional manner. I will not share any personal information with a pupil (including personal phone numbers or email address). Nor will I request or respond to any personal information from a young person unless it is appropriate as part of my professional role.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- I will lock my screen or log off my computer should I leave it unattended.
- I will not allow a third party to access my work emails on my mobile phone or tablet

6. SAFE & SECURE ACCESS TO TECHNOLOGIES

The school and the local authority have the responsibility to provide safe and secure access to technologies:

- When I use my personal handheld / external devices in school (PDAs / laptops / mobile phones / USB devices etc.), I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. As far as I am able, I will ensure that when connecting these devices to school ICT systems, they are using up to date Operating Systems (e.g. latest versions of Android / iOS) and protected by up-to-date anti-virus software where applicable.
- I will not save any personal data to my personal computer.
- I will not use my personal WhatsApp accounts to share organisational data, such as student data, staff information, or any other confidential school-related details.
- I will only use the recommended apps on my personal device for accessing data\emails via Office 365 or G-Suite.
- I will encrypt (Password Protect in most cases) my personal device if I use it to access school personal data or Office 365\G-Suite apps.
- I will inform the school's **Head Teacher or other person appointed by the Head Teacher/DPO** if my personal device e.g. phone or tablet is lost or stolen should it contain any school personal data.
- I will immediately report any Internet content that is not filtered that I suspect could be inappropriate.
- I will delete personal data according to the school's retention policy.
- I will not use personal email addresses for work-related purpose.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.

- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not upload, download or access any material which is illegal or inappropriate or may cause harm or distress to others (e.g. child sexual abuse images, criminally racist material, adult pornography etc.). I will not use any programmes or software that might allow me to bypass the filtering / security systems intended to prevent access to such materials.
- I will not install or attempt to install programmes of any type on school systems, nor will alter computer settings, unless this has been authorised.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Protection Policy. Where personal data is electronically transferred outside the secure school network, it must be encrypted.
- I will immediately report any damage or faults involving equipment or software; however, this may have happened.

7. INTERNET FOR PROFESSIONAL OR SCHOOL SANCTIONED PERSONAL USE

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

8. SYSTEM SPECIFIC GUIDELINES & PROCEDURES

Use of Electronic Whiteboards and Screensharing:

- I understand that electronic whiteboards should be used in a manner that upholds the school's standards of professionalism and respect.
- I will ensure that any content displayed or written on electronic whiteboards during lessons or meetings is appropriate for the intended audience.
- I will not save or store sensitive information displayed on the whiteboard without the necessary permissions or safeguards in place.
- When using interactive features, I will ensure that student data and privacy are protected at all times.
- When sharing the screen of my device (laptop, tablet, work phone etc.) to the electronic whiteboard, I will ensure that only the necessary applications or windows are visible to avoid unintentionally sharing sensitive or personal information. This also applies to screensharing during online remote lessons or meetings.
- I will be vigilant and ensure that any notifications or pop-ups that may contain personal or sensitive information are disabled before sharing my screen to the electronic whiteboard. This also applies to screensharing during online remote lessons or meetings.
- I will ensure that any shared content displayed on the electronic whiteboard or shared during online remote lessons or meetings, upholds the school's standards of professionalism and respect.

9. SCHOOL'S MANAGEMENT INFORMATION SYSTEM (MIS)

- I understand that the school's MIS contains sensitive data and information pertinent to the functioning of the school.
- I will only access the MIS with the appropriate permissions and for legitimate school-related purposes.
- I will not share my MIS login credentials with anyone and will ensure that I log out after each session.

- I will ensure that I do not display or share information from the MIS with individuals that are not authorised the access the data (for example, by displaying the MIS on classroom screens or electronic whiteboards).
- I will immediately report any suspected breaches or unauthorized access to the MIS to the school's IT department.
- I will use multi-factor authentication, where available, to enhance the security of my access to the MIS.

10. SCHOOLS SAFEGUARDING SYSTEM

(e.g. CPOMS, MyConcern, Provision Map)

- I acknowledge the sensitive nature of data within the school's safeguarding systems and will handle this information with utmost care and discretion.
- I will ensure that I only access these systems for legitimate safeguarding-related activities and will avoid unnecessary browsing or querying of data.
- I will not share my login credentials for safeguarding systems with anyone.
- I will ensure that I do not display or share information from the Safeguarding System with individuals that are not authorised the access the data (for example, by displaying the MIS on classroom screens or electronic whiteboards).
- Multi-factor authentication should be used when accessing these systems to ensure the highest level of security.
- Any suspected breaches, mishandling, or unauthorized access to these systems should be reported immediately to the designated safeguarding lead.

11. DECLARATION

<u>I understand that I am responsible for my actions in and out of school:</u>

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action and in the event of illegal activities, the involvement of the police.

I have read and understand the above and agree to use the school ICT systems both in and out of school and my own devices (in school and when carrying out communications related to the school) within these guidelines.

School:

Signed:

Print name:

Date:

POLICY HISTORY

Date	Summary of Change	Contact	Policy Implementation Date	Review Date
26/09/2024	Text updated in section 'The school and the local authority have the responsibility to provide safe and secure access to technologies' to prohibit the sharing of organisational data via personal WhatsApp Accounts.	SchoolPro TLC	Pending Committee Approval (October 2024)	October 2026