WILDRIDINGS PRIMARY SCHOOL

Staff and Volunteers

Acceptable Use Policy

		Signature	Date
Headteacher	**Mr Paul Chandler**		

Reviewed by Headteacher	**6th September 2023**
Next Review	**October 2023**

Staff and Volunteers
Acceptable Use Policy

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.

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.

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.

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.
- I understand that this agreement also applies to use of school ICT systems out of school (e.g. laptops, email, VLE etc.).
- 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. My password will contain upper, lower, numeric and special characters.
- I will immediately report any illegal, inappropriate or harmful material or incident, to the appropriate person in school.
- 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 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) it will not be possible to identify pupils by their full 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 shred all paperwork that contains details that could be deemed as a GDPR breach.

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

- When I use my personal hand held / 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.
- If accessing school emails on my mobile phone I will register my mobile phone with 'Find my phone' which will enable me to block my phone if lost or stolen. See Appendix 1.
- I will also follow any additional rules set by the school about such use.
- USB devices are allowed to be used in school but only to transfer resources. No personal data is to be stored on a USB drive. I will ensure that when connecting these devices to school ICT systems, they are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- 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 try to 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 try to use any programmes or software that might allow me to bypass the filtering / security systems intended to prevent access to such materials.

Unless I have permission, I will not try to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- I will not install or attempt to install programmes of any type on school systems, nor will I try to alter computer settings, unless this has been authorised by the school ICT Technical Support.
- 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. Documents will be password protected and an email or phone call will be made 5 minutes later with the password.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

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).
- I understand that I am responsible for my actions in and out of school:
- 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.

Signed …….. Print name…….

Date……..

ALL STAFF

Most of you generally have an apple or android mobile device, both of which support the office 365 app. In the event that you lose your phone you MUST follow the steps below:

- Staff to contact a senior member of staff immediately.
- Office 365 Administrator (Liz or Tina), locks or changes password. There should be an option to sign out of all other devices.
- Remotely lock or wipe the device
  - Android https://support.google.com/accounts/answer/6160491?hl=en
  - Apple https://support.apple.com/kb/PH2701?locale=en_GB

THESE MUST be installed onto your phones if you don't already have a google account set up. Please try this out and ask someone if you are unsure.

- Record the event in your data breach log and complete a data breach report.
- Senior member of staff to contact the DPO if they suspect this should be reported to the ICO and/or data subjects within 72 hours of becoming aware of the incident.

Staff mobile phone record

Name	Device	Device security enabled (Face ID/Password/Pin/Fingerprint Scanner/None)	Find my phone/device enabled (Yes/No/Don't know)	Declaration: I will inform the school if/when I use a new mobile device to access school data (tick)	Signature