POLICY - STAFF AND VOLUNTEER ACCEPTABLE USE OF ICT, AND PORTABLE DEVICES

_____

This policy should be read in conjunction with Data Protection Policy and Safeguarding Plan

School 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 information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

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

Signed: …….. Chair of Governors

Signed: …….. Headteacher

Review: September 2022

Acceptable use Of ICT Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of ICT. 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 the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, VLE etc) out of school.
- I understand that the school ICT systems are primarily intended for educational use.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident; I become aware of, to the appropriate person.

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

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- **I will not allow any other member of staff or student to access my network login on any of the school equipment, failure to comply with this will lead to disciplinary procedures.**
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. (See Guidance for Safe Working Practice).
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc) in school, 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. I

will ensure that any such devices 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 materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) 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 a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies or under the instruction of the ICT team
- 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 / LA Personal Data Policy. Where personal data is transferred outside the secure school network, it must be encrypted.
- Remote learning methods are not to be used until rolled out to staff by the school ICT team with instructions and guidance
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- 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 NOT to use my own technology for recording/photographing students.

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. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

Portable IT Devices

Equipment issued by Crowdys Hill School to a member of staff is subject to the following conditions:

1. The equipment remains the property of Crowdys Hill School at all times and must be returned to the school at the end of the lease agreement or contractual period. The equipment nominated above is the sole responsibility of the named individual.

   All school laptops which are being taken out of school need to be encrypted with PIN or Password, this encryption should not be suspended or switched off. Mobile devices/tablets (including personal devices) which have school email set up will need to be password/PIN protected.

2. Maintenance of the equipment is the responsibility of the ICT support department. All maintenance issues must be referred to the ICT support department, through the usual channels.

3. From time to time, it will be necessary for the ICT support department to perform software updates and maintenance for which the equipment must be made available in school when requested.

4. All installed software MUST be covered by a valid license agreement held by the school. No member of staff must install any software that does not have a valid license agreement.

5. All software installation MUST be carried out by the ICT support department in accordance with the relevant license agreements.

6. When equipment is to be used to access the internet other than by the school broadband connection, users MUST ensure that spyware protection software, anti- virus software and a firewall are installed. Connection to the internet should not be by wireless

router, unless the wireless connections signal it is fully encrypted and password protected. Please ask a member of the ICT team if you are unsure.

7. No software should be removed, uninstalled or disabled under any circumstances. Any software problems should be reported through the usual support channels.

8. Protective software must be updated regularly. For laptop computers, it will be necessary to connect them to the school network to update the **group policies and software updates/changes** (The school now is using Sophos Central which is cloud based and will update on any internet connection) This should be done regularly with updates continuously added automatically during normal in school use at least once a week.

9. All user profiles are redirected to server, so data is backed up with the scheduled server backups . The school is not responsible for personal files outside of this provision, users should store on other external media where necessary.

10. The ICT support department cannot be held responsible for loss of data in the event of either a hardware or software failure or user error.

11. Internet usage is subject to the school e-Safety Policy Connection activity may be logged and monitored for safeguarding and security purposes

12. School equipment should not be used to access any web-based e-mails apart from Outlook **online**(school email) as the ICT support department is unable to offer any guarantees regarding the availability, performance, reliability or safety of such services.

13. If school equipment is to be used by anyone other than the member of staff responsible for it, that user must have a separate account set up by the ICT Support Department. The laptop must remain in the users possession at all times and remains the user's responsibility.

14. Using a VPN to access internal resources comes with responsibilities to uphold network security, as well as to safely and equitably use school resources. All computers connected via VPN must use the most up-to-date antivirus software that is the corporate standard; this includes personal computers. Users must ensure that their personal computers have the most up-to-date security patches applied (e.g. via Windows Update)

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.

Staff / Volunteer Name: ……

Signed: …….. ……. Date: ….....