CLT Staff and Volunteer Acceptable Use Policy

School Policy

This Acceptable Use Policy reflects the school Online Safety and GDPR policies. The school will ensure that staff and volunteers will have access to technology to enable efficient and effective working including enabling learning opportunities for pupils, research, administration and management and will, in return, expect staff and volunteers to agree to be responsible users.

This policy has been drawn up to protect all parties – students, staff, volunteers and the school. Professional standards should be maintained to safeguard the reputation of the school, and to ensure the safety of all.

In this policy, the term 'computer' refers to ANY electronic device, school or personally owned, used for school / work.

Scope of Policy

This Acceptable User Policy (AUP) policy applies to staff, volunteers and guests who have access to and are users of school technology systems, school related use of technology systems outside of school, and make use of social networks personally or professionally.

My Responsibilities

I agree to:

- read, understand, sign and act in accordance with the school Online Safety Policy and the school GDPR policy
- report any suspected misuse or concerns to the Online Safety Lead / Designated Safeguarding Lead as appropriate
- monitor technology activity in lessons, extracurricular and extended school activities (including Online / Remote Learning) including awareness of any access to extremist views
- model the safe and effective use of technology
- be mindful of the additional safeguarding considerations required if delivering Online / Remote Learning
- demonstrate consistently high standards of personal and professional conduct, especially in relation to use of social networks, making sure this is in line with school ethos and policies, especially during Critical Incidents
- use the system in a safe, legal and business appropriate manner
- not use computers for private or personal use during timetabled lessons and / or in the presence of students
- be open, honest and transparent about my conduct

Education

I agree to:

- provide age-appropriate online safety learning opportunities as part of a progressive Online Safety curriculum within the RSE Curriculum, which complements the Computing Curriculum, and reinforce the learning throughout the school's curriculum
- respect copyright and educate the pupils to respect it as well
- teach about the need for responsible and caring language when communicating with others

Training

I agree to:

- participate in online safety training
- undertake relevant CsPD if I identify an opportunity to improve my professional abilities and seek support if required

Online bullying

I agree to:

- ensure the school's zero tolerance of bullying. In this context, online bullying is seen as no

different to other types of bullying
- report any incidents of bullying in accordance with school procedures

Sexting
- I will secure and switch off the screen of any device discovered with a sexting or sexual harassment image, without showing others, and immediately report it to the Designated Safeguarding Lead
- I will not investigate, delete, share or resend the image

Prevent
- I will continually develop children's ability to evaluate information accessed online.
- I will follow the agreed reporting procedure where children are purposefully searching for inappropriate sites or inadvertently accessing inappropriate sites.

Technical Infrastructure

I understand that the school will monitor my use of computing devices and the internet. Unless I have permission, I will not try to by-pass any of the technical security measures that have been put in place by the school which include:
- the proxy or firewall settings of the school network
- not having the rights to download software on a school computer without prior consent (A request Form for this will be on the Communication Hub)
- not using removable media e.g. memory sticks unless approved by 2IT. (OneDrive & Teams should be used instead)

Passwords
- I will only use my own, unique usernames and passwords or multi-user accounts I am authorised to use
- I will never log another user onto the system using my login or share my passwords
- I will not store passwords using 'auto-fill' settings on shared devices
- I will immediately reset my password if I think it has been compromised and seek help
- I will always ensure I log out of, or lock, any computer I leave unattended

Filtering
- I will not try to by-pass the filtering system used by the school
- If I am granted special access to sites that are normally filtered I will not leave my computer unsupervised
- I will report any filtering issues immediately

Reporting problems with the computer system
- I will report all problems with the school IT Support team by emailing helpdesk@clevedonlearningtrust.org.uk
- If I suspect a computer has been affected by a virus or other malware, I will report this to a member of the IT Support Team immediately
- If I have lost documents or files I will report this as soon as possible

Data Protection
- I understand my responsibilities towards the data protection regulations and will ensure the safe keeping of personal and sensitive personal data at all times in accordance with the school and Trust GDPR policies.

Use of digital images, video and sound
- I will follow the school's policy on using digital images, video and sound, especially in making sure that only those pupils whose parental permission has been given are published
- I will not use personal devices for taking or sharing digital images or sound unless approved by the Head Teacher & DSL

Communication
- I will be professional in all my communications and actions when using school technology systems including Teams messages and chat in Teams Meetings.
- I understand that I need to be open and transparent in all my communications

Email

- I will use the school provided email for all business matters
- I will ensure all email correspondence is professional and business like, as email has the same permanence and legal status as paper documents, and may be subject to disclosure obligations in exactly the same way. I will be cautious sending both internal and external emails.
- I will ensure emails are sent only to students via their school email address and not to a personal email address (even when replying to emails from private addresses) except in exceptional circumstances where it is not possible to use their school account. In such circumstances I will ensure that a parent/carer is ALWAYS copied into the email.
- I understand that email is not a secure communication method. It can easily be copied, forwarded and archived.
- I will not send personal data via email and will seek advice if unsure
- I will ensure all school emails I send have a signature containing my name, job title and the name of the school. (A template for which can be supplied but I acknowledge it is my responsibility to set up and maintain)
- 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 programs). If I receive anything I am suspicious of I will immediately delete without opening and permanently delete from my deleted items folder.
- I will not use my school email address for any non-school purpose, including registering on websites that are not for school

Online/Remote Learning

- I will check with 2IT/ CLT IT / Data Protection Officer before I use sites/apps with learner log ins to ensure that any pupil personal data is being held securely
- I understand that any digital communication with staff, pupils, parents or carers is open, transparent and professional in tone and content
- I will ensure I have read the Remote Learning Policy and the relevant DfE guidance

Social Media and Personal Publishing

- I will ask permission before I use social media e.g. blogs, social networks or online communication tools with pupils or for other school related work. These will never be my personal accounts
- I will follow the online safety policy concerning the personal use of social media, never publishing disparaging or harmful comments or expressing extreme views. These are considered to bring the school into disrepute
- I will not post any comments about the school, any pupil, employer or colleagues on any personal social networking and publishing accounts which may bring the school or Trust into disrepute
- When there is a Critical Incident, I will not post any comments online

Personal devices

- I will check that any personal devices I have in school are pin code or fingerprint protected and not discoverable by third parties. Airdrop may be used but should only be turned on while collecting in work.
- I will not be required to use my personal devices to call pupils or parents. If exceptional circumstances require me to use my device I will either use Teams to call or withhold my number.
- I am responsible for any use of my own mobile data during agreed times and ensuring that my use complies with the school's online safety policy

Reporting incidents

- I will report and record any incidents relating to online safety to the Online Safety Lead / Designated Safeguarding Lead and check this has been recorded and actioned
- I understand that in some cases the Police may need to be informed
- I will report any abuse of any part of the computer system to the IT Support team immediately

Unacceptable behaviour

Examples of unacceptable behaviour include, but are not limited to:

- using, transmitting or seeking inappropriate, offensive, pornographic, vulgar, suggestive, obscene, abusive, harassing, threatening, racist, sexist, homophobic or defamatory language or materials
- making ethnic, sexual-preference or gender-related slurs or jokes
- storing inappropriate or illegal content on a school owned computer or a computer in school

Privacy

The use of school ICT systems, including email accounts and storage provided for your use, may be subject to monitoring by the school to ensure compliance with this Acceptable Usage Policy and applicable laws.

In the interests of safeguarding, the school reserves the right to inspect ANY electronic device on school premises whether owned by school or the individual.

Sanctions and Disciplinary procedures

- I understand that there are regulations in place when pupils use technology and will apply sanctions if they do not follow the rules
- I understand that if I misuse the School technology systems in any way then there are disciplinary procedures that will be followed by the school

---

CLT & St Nicholas Chantry School – Staff and Volunteer AUP
September 2022

I have read and understand the full School online safety policy and agree to use the school technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) in a responsible and professional manner as outlined in that document.

Staff/Volunteer Name: ……

Signed: ……

Date: ……