TRINITY SCHOOL'S ACCEPTABLE USE POLICY FOR STAFF

"Everyone who works with children should do what is in the best interest of the child"
Article 3 United Nations Rights of the Child

Trinity School has provided computers for use by staff as an important tool for teaching, learning and administration of the school. Use of school computers, by both members of staff and pupils, is always governed by the following policy. Please ensure that you understand your responsibilities under this policy and direct any questions or concerns to the computing coordinator in the first instance.

The purpose of the policy is to ensure the school network is operated safely and all users are safe. It refers to our school network and to the use of mobile technologies within it and explains the behaviours, which are acceptable and unacceptable within our school.

This document outlines the key points of our AUP (Acceptable User Policy). It has been written to ensure all adults working within school are aware of the rules, risks and procedures we operate under our full AUP, issued by the department.

All members of staff have a responsibility to use the school's computer system in a professional, lawful and ethical manner. Our AUP must be fully complied with at all times. All users of the school network should note that it is monitored on a daily basis. Whilst our network and systems are organised to maintain the most secure environment possible it is your responsibility to make sure the children you are directly working with are safe.

As an adult working in school you may be the first point of contact in dealing with incidents of IT misuse or abuse. Every such incident must be reported to the Class Teacher who will then follow the school's procedures.

Your key responsibilities are:

- Maintaining an appropriate level of professional conduct in your own internet use within the school.
- Developing and maintaining knowledge of internet safety issues, particularly with regard to how they might affect children.
- Implementing our school AUP through effective classroom practice.
- Reporting any instances of ICT misuse to the Class Teacher who must report it to the E-Safety Coordinator in line with our school AUP. If the Class Teacher is suspected of being involved, report directly to the E-Safety Coordinator or Head Teacher.
- Supporting pupils who experience problems when using the internet, working with the Class Teacher.
- Using the internet and ICT facilities to ensure that internet safety is not compromised e.g. evaluating website in advance of classroom use, using child oriented search engines.
- Embedding internet safety messages wherever possible.
- Following the school rules relating to acceptable use of our ICT equipment and other mobile technologies.
- Copies of our rules for pupil use of the network are displayed around the school. Please ensure you have read them and make sure the pupils you work with adhere to them.

School ICT Network

The school Network and associated services may be used for educational purposes only.

- All adults working within the school must log on to the computers using their own username and password only. Passwords need to be kept a secret. If an adult needs to leave their computer, they have to lock the computer to prevent others from using their account by pressing "Ctrl, Alt and Delete".
- All adult iPads must have a 6-figure passcode.
- Any supply teachers to the school must obtain a username and password from the school administrator for use on that day.

Software and Downloads

- All users of the network must virus check any USB device storage devices before using on the network.
- If users need a new program installing onto the computer, the CYPES Department IT team will be asked to this for us.
- Copyright and intellectual property rights must be respected when downloading from the internet.

Personal Use

The school recognises that occasional personal use of the school's computer is beneficial both to the development of ICT skills and for maintaining a positive work-life balance. Such use is permitted, with the conditions that such use:

- Most comply with all other conditions of the AUP as they apply to non-personal use, and all other school polices regarding staff conduct.
- Must not interfere in any way with your other duties or those of any other member of staff.
- Must not have any undue effect on the performance of the computer system; and
- Must not be for any commercial purpose or gain unless explicitly authorised by the school.

Personal use is permitted at the discretion of the school and can be limited or revoked at any time.

Email

- All members of staff with a computer account in school are provided with a school email address for communication both internally and with other email users outside of school.
- These accounts must only be used for school-related emails.
- Emails should be written carefully and politely using appropriate language.
- Email attachments should only be opened if the source is known and trusted.
- I will ensure that all my login credentials (including passwords) are not shared with any other individuals. If I think someone has learned my password then I will change it immediately and/or contact the ICT technician.

Images/Videos

Class teachers will refer to parental consent forms before uploading images/videos to the website. No identifiable images can be used on Facebook posts.

- Adults may only take images/videos of students on their school iPad. No personal phones or devices may be used for images/videos of students.
- Photos and videos will be deleted or transferred to the school network at the end of each academic year or before.

Network Protocol

- School computer and Internet use must be appropriate to a pupil's education or to staff professional activity.
- Respect other people's material and do not corrupt, interfere with or destroy them.
- Do not open other people's files without expressed permission.
- When working with personal data ensure that the data is secure.

Internet Usage

- Pupils must be supervised always when using the internet.
- Activities should be planned so "open" searching is kept to a minimum. All websites should be viewed by the teacher prior to showing/using with pupils.
- When searching the internet with pupils, adults should encourage the children to use "child safe" search engines.
- The use of social networking sites, public chat rooms and messaging systems (e.g. Facebook, Messenger, X) are not allowed from school networks.
- Use of the internet on school devices and the network machines should be for educational purposes only.

Use of Social Networking Sites and Online Forums

Staff must take care when using website and social media sites, even when such use occurs in their own time on their own computer at home. When using these sites:

- You must not add a pupil to your "friends list", accept or invite them to be friends with you, even if that pupil has subsequently left the school.
- You should not add a parent to your "friends list" unless you are friends with them outside the school community.
- You must ensure that personal information is not accessible via "Public" setting, but ensure it is to a "Friends only" level of visibility.
- You must not contact any pupils or parents privately via social networking sites, even for school related purposes.

Remember that damage to professional reputations can inadvertently be caused by quite innocent postings or images. You will need to ensure that any private social networking sites/blogs that you create or actively contribute to are not to be confused with your professional role in any way.

Staff should also take care when posting to any public website (including online discussion forums or blogs) that their comments do not harm their professional standing or the reputation of the school – even if their online activities are entirely unrelated to the school.

- Unless authorised to do so, you must not post comments on website that may appear as if you are speaking for the school.
- You should not post any material online that can be clearly linked to the school that may damage the school's reputation.
- You should avoid posting any material clearly identifying yourself, another member of staff or a pupil, that could potentially be used to embarrass, harass or defame the subject.

Use of your own Equipment

- Personal tablets or phones should not be used for school purposes
- During teaching time, mobile phones should be turned off or put on silent mode and stored in a cupboard, bag or locker away from the children.
- Adults are allowed to access their personal phones on breaks, lunch times and after school in designated areas e.g. staff room or teachers room (safe, suitable places where the children are not present).
- It is forbidden to take photographs/ videos of the children on personal mobiles.
- You must not connect personal computer equipment to the school computer equipment without prior approval from an ICT Technician, without the exception of storage devices such as USB memory sticks.

Supervision or Pupil Use

- Students must always be supervised when using school computer equipment. Supervising staff need to ensure that students and parents have signed the Student AUP and that they are attached to the front cover of their computing book. When arranging use of computer facilities for pupils, you must ensure supervision is available.
- Supervising staff are responsible for ensuring that the student AUP is enforced.
- When iPads are taken out of school for use on school trips, the class teacher must check that all iPads have a 4-figure passcode.

Reporting Problems with the Computer System

- You should report any problems that need attention by email to the IT Technical and copy in the Subject leader for ICT or Headteacher. All ICT issues will need to be reported to the Department via the Education IT Network.
- If you suspect your computer has been affected by a virus or other malware, you must report this to the ICT Technician immediately.
- If you have lost documents or files, you should report this as soon as possible. The longer a data loss problem goes unreported, there is less chance of your data being recoverable.

Reporting Breaches of this Policy

All members of staff have a duty to ensure this Acceptable Use Policy is followed. You must immediately inform the Computing coordinator or Headteacher, of abuse of any part of the computer system. You should report:

- Any websites accessible from within school that you feel are unsuitable for staff or pupil consumption.
- Any inappropriate content suspected to be stored on the computer system. This may be contained in email, documents, pictures etc.

- Any breaches, or attempted breaches, of computer security, or
- Any instance of bullying or harassment suffered by you, another member of staff, or a pupil via the school computer system.

Any breach of this policy could be a breach in staff contracts and could lead to disciplinary proceedings.

I have read, understood, and agree to comply with the Acceptable Use Policy.

Signed: _____ Date: _____

Print Name: _____