Trinity School's Acceptable Use Policy for Adults

Trinity School provides 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 governed at all times by the following policy. Please ensure that you understand your responsibilities under this policy, and direct any questions or concerns to the computing subject leader 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. It has been written to ensure all adults working within school are aware of the rules, risks and procedures we operate under.

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 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 IT misuse to the Class Teacher who must report it to the E-Safety Subject leader in line with our school AUP. If the Class Teacher is suspected of being involved, report directly to the E-Safety Subject leader or Head Teacher.
- Supporting pupils who experience problems when using the internet, working with the Class Teacher.
- Using the internet and IT facilities to ensure that internet safety is not compromised e.g. evaluating websites in advance of classroom use, using chid oriented search engines.
- Embedding internet safety messages wherever possible.
- Following the school rules relating to acceptable use of our IT equipment and other mobile technologies.
- Copies of our AUP for pupils are displayed on the front cover of their computing books. 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.

Passwords

- 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 or a device, a DPIA much be completed on the EDU-Information Governance Teams Sharepoint and request must be emailed to the IT team by one of the leadership team of Mrs Racjan.
- Copyright and intellectual property rights must be respected when downloading from the internet.

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.
- E-mail should be written carefully and politely using appropriate language.
- E-mail attachments should only be opened if the source is known and trusted.
- Login credentials (including passwords) should not be shared with any other individuals. If anyone thinks someone knows their password, they should change it immediately and/or contact IT through the Leadership team.
- Any unsuitable communications received must be reported to the e-safety subject leader immediately.

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 of 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.
- When permission has been received from parents, staff may upload images and videos of children onto their Google Classroom site.

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 at all times 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.
- 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 websites 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.

- 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 should avoid contacting any pupil privately via social networking site, 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 anyway.

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 websites 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

- 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 mobile phones.
- You must not connect personal computer equipment to school computer equipment without prior approval from IT Technician, without the exception of storage devices such as USB memory sticks.

Supervision of Pupil Use

- Students must be supervised at all times when using school computer equipment. Supervising staff needs 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 to the Computing subject leader.
- If you suspect your computer has been affected by a virus or other malware, you must report this to Computing subject leader immediately.
- If you have lost documents or files, you should report this as soon as possible. The longer a data loss problem goes unreported, the less chances 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 subject leader or the Head Teacher, of abuse of any part of the computer system. In particular, 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.

All reports will be treated confidentially.

Electronic Devices - Searching & Deletion

In accordance to 'The Education Act 2012' school has the right to search and or delete anything from personal devices if they believe illegal or suspicious activity is taken place.

Review and Evaluation

This policy will be reviewed regularly and in response to any changes affecting the basis of the original risk assessment, for example: significant security incidents, new vulnerabilities and significant changes to the organisation or technical infrastructure. Changes to this policy will be communicated to all staff.

I have read, understood and agree to comply with the AUP:

Signed: _____ Date: _____

Print Name: _____