NCEAT Trustees 

Digital Device, Internet and Systems Acceptable Use Agreement

ICT and the related technologies such as Pcs, email, internet, school admin/data systems and mobile devices are an expected part of our daily working life in the Trust. This policy is designed to ensure that all trustees are aware of their responsibilities when using any form of ICT. All trustees are expected to sign this policy and adhere at all times to its contents.

To ensure that safety is not compromised:

**You must:**

* If you have cause to use Trust ICT equipment at any time then this must be for Trust purposes only
* Treat the trust ICT equipment with care
* Keep your password safe and report any password that is compromised
* Only store trust admin related files and information on Trust devices and software systems. (Google drive)
* Only store personal student/trust staff information on an Trust device, the Trust Google Drive or encrypted USB key/drive
* Only install / use licensed or open source software that is work related and has been checked by the technicians
* Report any misuse of ICT equipment/systems or inappropriate content to either the Network Manager, CEO or the Child Protection officer depending on the context
* Ensure that any digital communication is addressed and sent to the correct person/people
* Ensure that any personal devices used to access Trust emails and/or data systems are password or pin protected and the device account is not used by anyone other than yourself
* Ensure all devices are locked when unattended
* When hosting a video conference on behalf of the Trust you must use Google Meet from your Trust email account. You are free to be a participant of other systems such as Zoom or Microsoft Teams.

**You must NOT:**

* Access or try to access chat rooms, forums, messaging, pornography, social media or gambling sites that have not been ratified by the Trust using Trust systems or equipment.
* Access/download or try to access/download any illegal material for example movies, music etc using trust systems or equipment.
* Actively bypass or attempt to bypass school security measures including the use of proxy bypass websites
* Bring digital material into school that has not been virus checked

Use The Trust Google Drive/Email system to share/distribute files or information that is illegal, pornographic or may cause offense or distress

* Log into hardware or software with a user name or password that is not your own; or use another person’s account at any time
* Store files on Trust devices and systems that are not related to Trust work
* Use material for Trust work without permission from the copyright holder / owner
* Deliberately damage the computer equipment or use the network in a manner that will prevent others using it
* Use ICT equipment for fraudulent purposes
* Allow your laptop /assigned device or Trust software system to be used by any person not employed by the Trust at any time in or out of the Trust buildings
* Use any ICT equipment to harass, bully, abuse or otherwise distress any individual inside or outside the Trust
* Use Trust ICT equipment / Internet for recreational use
* Accept friend requests / request friend status from students, parents or carers on social media on a Trust account
* Communicate electronically with students/parents/carers other than through Trust systems; this includes use of personal mobile phones
* Use non Trust equipment e.g. personal mobile phones/tablets to take still pictures of or stream/make videos of students at any time.

**You should be aware that:**

* We will check your network user area / Google Drive regularly to ensure correct and appropriate usage
* You are totally responsible for your own user space and files created or saved on Trust devices/network drive or Google Drive, any unsuitable material found is your responsibility
* Any material in your user area / Google drive that is not work related can be deleted at any time without warning
* While the Trust runs regular backups, you are advised to maintain encrypted off site backups of your own work
* Your ICT use both in and out of school will be monitored when using Trust devices and software systems
* The Trust is not liable for any fraudulent or criminal activity as a result of ecommerce undertaken by yourself
* Any social networking web sites used should be secured with the highest security permissions appropriate at all times

**Consequences of violations:**

* Minor infringements will be reported to the CEO and appropriate action taken.
* When applicable police or local authorities will be involved.

 **Reporting of violations**:

* ALL violations witnessed should be discussed with the appropriate CEO or Network Manager.
* You are required to sign and abide by this Acceptable Use Agreement before using Trust equipment or software systems.

This policy may be updated during your time in school. The current agreement can be viewed at www.ncea.org.uk

I agree to abide by the rules set out in this Acceptable Use Agreement

Signature ………………………………………………………………………

Print name……………………………………….…………………………….

Date …………………………………………………………………………….

Summary of Good Practice Guidelines

Appropriate

1. Set your privacy settings for any social networking sites to ensure only the people you want to have sight / access to the contents. Keep these updated. The default settings for most social networking sites are set to open access where anyone can see everything.
2. Ensure your mobile phone (any technological equipment) is password/PIN protected. This will ensure that other people can’t use your equipment.
3. Make sure that all information about you that is publicly available is accurate and appropriate – think particularly about whether photographs / stories that you may have posted in your personal life are appropriate for a person with a professional life and a reputation to lose. If you don’t want it to be public, don’t put it online.
4. Remember that online conversations may be referred to as ‘chat’ but they are written documents and should always be treated as such. Be mindful about how you present yourself when you are publishing information about yourself or having ‘conversations’ online.
5. Make sure that you are aware of your organisation’s policy regarding the use of both organisational and personal digital equipment and the consequences of misuse. Breach of the policy can result in capability/disciplinary actions by your employer, professional body and criminal proceedings by the police.
6. Err on the side of caution. If you are unsure who can view online material, assume that it is publicly available. Remember – once information is online you have relinquished control of it. Other people may choose to copy it, to edit it, to pass it on and to save it.
7. Switch off / make secure any Bluetooth capability any device may have installed as standard. Bluetooth allows another person to have access to your equipment – they can then pretend to be you.
8. Always be aware that technology is constantly upgrading and improving. When you receive any new equipment (personal or private) make sure that you know what features it has as standard and take appropriate action to disable/protect yourself and your data.

Inappropriate

1. Give your personal information to students / parents / carers. This includes personal mobile phone numbers, social networking accounts, personal website/blog URLs, online image storage sites, passwords/PIN numbers etc.
2. Use your personal mobile phone to communicate with students / parents / carers either by phone calls, text, email, social networking sites.
3. Use the internet or web based communication to send personal messages to students / parents / carers.
4. Share your personal details on a social network site with students / parents / carers. This includes accepting them as friends. Be aware that belonging to a ‘group’ may give ‘back door’ access to your page even though you have set your privacy settings to friends and family only.
5. Use your own digital camera / video for work. This includes integral cameras on mobile phones.