?:

Computer/Mobile Device Use and Online Policy - Staff

Review Summary

Adopted:	**March 2018**
Review Cycle:	**Bi-annual**
Last Review:	**May 2020**
Next Review:	**May 2022**

1. Introduction

1.1. The IT infrastructure is owned by the Trust and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management. This policy has been drawn up to protect all parties – the pupils, the staff, the schools and the Trust.

1.2. If a member of staff breaches this policy, then disciplinary action may be taken.

2. Protocol for Use of Trust Mobile Technology Devices.

2.1. Users of Trust mobile technology devices are responsible for the following:

a. Ensuring the mobile device is protected by a password or pin code;
b. Returning the mobile device to the IT team when it is no longer required;
c. Only using official stores for installing mobile apps e.g. Microsoft store, Apple store, Google Play;
d. Not changing security settings or amending configuration files. This includes disabling passwords, pin codes and any installed security programs (e.g. Anti-Virus applications);
e. Notifying the IT helpdesk in the event that the mobile device is lost or stolen.

2.1 When using your Trust mobile device:

f. Turn it off and put it in an appropriate carrying case when travelling;
g. Take care when connecting the network cable and seating the mobile device on a docking station as the connections can be easily damaged;
h. Keep all drinks and any other liquids away from your device. Any spillage on the device can result in data loss and expensive repairs;
i. Do not leave it in full view in a vehicle even for a short period of time. It must be locked in the boot, when the vehicle is left unattended and not left in the vehicle overnight, even in a locked boot;
j. Lock it away in a drawer or cupboard when left unattended on site for an extended period of time or over-night;
k. Never leave it unattended in public places even for a very short period of time;
l. If travelling by air, mobile devices must always be carried in the cabin and never checked in to the hold.

2.2 Installation of Software:

a. Submit a request to the IT helpdesk for the installation of academic or administrative software on the Trust's networks or on student IT facilities. This includes upgrades to packages already installed and applications to be developed in-house;
b. The request must include an adequate lead in time to allow the IT team to meet the request in the required timescale;

c. Software will only be installed on Trust computers or networks if there are the appropriate licences, and if its use is in accordance with its licensing rules;
d. Unless explicitly authorised, all Trust software is only for teaching and learning use, or for the purposes of the Trust's business and administration;
e. Staff and students who leave the Trust must remove all Trust software and data immediately.

3 Protocol for use of Personal Mobile Technology Devices

3.1 The purpose of this protocol is to prevent unacceptable use of mobile phones, camera-phones and other handheld devices by the school community, and thereby protect the school's staff and students from undesirable materials, filming, intimidation or harassment.

3.2 Should mobile technology devices be misused, there will be a negative impact on an individual's safety, dignity, privacy and right to confidentiality. Such concerns are not to be considered exclusive to children and young people, so the needs and vulnerabilities of all must be respected and protected.

3.3 It is to be recognised that it is the enhanced functions of many mobile technology devices that will give the most cause for concern; and which should be considered the most susceptible to potential misuse. Examples of misuse include the taking and distribution of indecent images, exploitation and bullying.

3.4 The school reserves the right to search the content of any mobile technology device on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying.

3.5 Personal mobile technology devices brought into school are the responsibility of the device owner. The Trust accepts no responsibility for the loss, theft or damage of these devices.

3.6 Staff must:

a. not use personal mobile technology devices to take photos or videos of students. They should only use work-provided equipment for this purpose;

b. ensure that any permitted images or files taken by personal mobile technology devices in school are downloaded from the device and deleted in school before the end of the day;

c. not use mobile technology devices in certain areas within the school site, e.g. changing rooms and toilets;

d. not use their own mobile technology devices for contacting children, young people or their families within or outside of the setting in a professional capacity. Staff will be issued with a school phone where contact with students, parents or carers is required;

e. switch off personal mobile technology devices or switch to 'silent' mode during the school day. Bluetooth communication should be 'hidden' or switched off and must not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.

f. Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide their own mobile number (by inputting 141) for confidentiality purposes.

3.7 Students can:

a. use mobile phones in specific learning activities under the supervision of a member of staff;

b. have a mobile phone for their own safety, where this has been requested by the parent;

c. Have their personal mobile technology device confiscated if this policy is not adhered to and will be held in a secure place in the school office. They will be released to parents or carers in accordance with the school policy;

d. not take personal mobile technology devices into examinations. Students found in possession of a personal mobile technology device during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.

e. contact his or her parents or carers, using a school phone, if the need arises. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office;

f. protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed via curriculum time and via assemblies in safe and appropriate use of mobile technology devices and will be made aware of boundaries and consequences.

4 Digital Communication

4.1 The following good practice must be followed:

a. Only contact pupils via school authorised mechanisms. At no time should personal telephone numbers, email addresses or communication routes via personal accounts on social media platforms be used to communicate with pupils;

b. Only contact parents and carers using school telephone numbers, email addresses and social networking sites that are set up for professional purposes

and approved by their line manager. It is prohibited for staff to use their personal contact details to contact parents and carers;

c. Any digital or written communication between staff and students or parents/carers must be professional in tone and content;

d. Any digital or written communication may be monitored and may be subject to a subject access request, therefore no digital or written communication can be considered private and confidential, therefore must always be written with this knowledge;

e. Any emails that are received which make a user uncomfortable and/or is threatening or bullying in nature should be reported to the line manager, e-safety co-ordinator or the designated safeguarding lead. Do not respond to the email.

5 E-Safety and Internet Use

5.1 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 use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

a. Access to illegal, harmful or inappropriate images or other content

b. Unauthorised access to, loss or sharing of personal information

c. The risk of being subject to grooming by those with whom they make contact on the internet

d. The sharing or distribution of personal images without an individual's consent or knowledge

e. Inappropriate communication or contact with others, including strangers

f. Cyber-bullying

g. Access to unsuitable video or internet games

h. An inability to evaluate the quality, accuracy and relevance of information on the internet

i. Plagiarism and copyright infringement

j. Illegal downloading of music or video files

k. The potential for excessive use which may impact on the social and emotional development and learning of the young person.

5.2 As with all other risks, it is impossible to eliminate these risks completely. It is therefore essential, through good educational provision, to build students' resilience

to the risks to which they may be exposed so that they have the confidence and skills to face and deal with these risks.

5.3 Staff must

a. not access pornography; neither should personal equipment containing pornographic images or links to them be brought into school;

b. not engage in inappropriate use of social network sites which may bring themselves, the school, school community or the Trust into disrepute. Ensure that suitably high security settings are adopted on any personal profiles;

c. exercise caution in their use of all social media or any other web-based presence that they may have, including written content, videos or photographs, and views expressed either directly or by 'liking' certain pages or posts established by others. This may also include the use of dating websites where staff could encounter students either with their own profile or acting covertly;

d. not link themselves with the school on any social network site they use unless with prior consent of the Head teacher;

e. not respond to negative comments posted online but bring this to the attention of the Headteacher;

f. must report to the Headteacher any contact by a pupil by an inappropriate route.

g. only take photographs/still images or video footage of pupils using school equipment, for purposes authorised by the school. Any such use should always be transparent and only occur where parental consent has been given. The resultant files from such recording or taking of photographs must be stored in accordance with the schools' procedures.

5.4 Staff are responsible for ensuring that:

a. they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices;

b. they have read, understood and signed the school guidance for 'Safer-working Practice for Adults who work with Children and Young People';

c. they report any suspected misuse or problem to the E-Safety Co-ordinator for investigation and action;

d. digital communications with students should be on a professional level and only carried out using official school systems;

e. pupils understand and follow the School Computer/Mobile Device & Online Safety Policy;

f. they monitor ICT activity in lessons, extra-curricular and extended school activities;

g. they are aware of e-safety issues related to the use of mobile technology devices and that they monitor their use and implement current school policies with regard to these devices;

h. in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

6 Unsuitable/Inappropriate Activities

6.1 Users shall not visit internet sites, post, download, upload, communicate or pass on, material and comments that contain or relate to:

a. offensive materials: child sexual abuse images, promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation, adult material that potentially breaches the Obscene Publications Act in the UK, racist material, pornography, promotion of any kind of discrimination, promotion of religious hatred, threatening behaviour;

b. using school systems to run a private business;

c. use of systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed;

d. uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions;

e. revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords);

f. creating or propagating computer viruses or other harmful files;

g. carrying out sustained or instantaneous high-volume network traffic; (downloading/uploading files) that causes network congestion and hinders others in their use of the internet.

6.2 This also applies to students' use of personal mobile technology devices to and from school and whilst on school premises.

7 Responding to Incidents of Misuse

7.1 Any apparent or actual misuse which appears to involve illegal activity, will be reported initially to the E-Safety Coordinator i.e.

a. child sexual abuse images
b. adult material which potentially breaches the Obscene Publications Act
c. criminally racist material
d. other criminal conduct, activity or materials

7.2 Actions will be followed in line with the school procedures, including reporting the incident to the police and the preservation of such evidence. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. Such incidents of misuse will be dealt with through the normal behaviour management policy.

8 Use of Digital and Video Images – photographic and video

8.1 When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. One important area is that they recognise the risks attached to publishing their own images on the internet e.g. on social networking websites.

8.2 Staff can take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.

8.3 Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute;

8.4 Students must not take, use, share, publish or distribute images of others without their permission.

9 Following Copyright Laws

9.1 The Copyright laws of the UK and other countries must not be infringed. Downloading material from the Internet carries the risk of infringing copyright. This applies to files, music, films, TV programmes, documents and software, which must be licensed.

9.2 Material illegally copied in this country or elsewhere and then transmitted to another country via the Internet, will also infringe the copyright laws of the country receiving it.

9.3 Any uploading or downloading of information through on-line technologies which is not authorised by the copyright owner will be deemed to be an infringement of her/his rights.

9.4 Users must not make, transmit or store an electronic copy of copyright material

10 Disposal of Trust IT, AV and Digital Equipment

Disposal of this equipment is governed by the WEEE directive and the Trust has clear guidelines that must be followed:

a. The disposal of all such equipment is arranged by the Trust IT Helpdesk, who will ensure that equipment is disposed of securely and safely, using a contractor who will dispose of the equipment in accordance with the required legal standard.

b. All data from the local hard disk must be deleted before the equipment is removed. The IT Helpdesk will advise whether the equipment can be reused elsewhere within the Trust.

c. Ensure your departmental asset register of equipment is updated to reflect any equipment being disposed of.

d. Devices which store data cannot be passed on to third parties as it is not possible to perform the necessary hard disk erase internally nor is it possible to transfer software owned by the Trust to a third party.

11 Policy Circulation

11.1 This Policy will be published on the Trust's website, circulated to every staff member as part of the induction process and is included within the staff handbook.

11.2 The Trustees are responsible for overseeing, reviewing and organising the revision of this Policy.

Adoption of the Policy

This Policy has been adopted by the Trustees of the Ted Wragg Multi Academy Trust**.**

Signed

(Chair of Trust)

Date: 04.06.20