Computer/Mobile Device Use and Online Policy - Pupils

Review Summary

Adopted:	**March 2018**
Review Cycle:	**Bi-annual**
Last Review:	**June 2022**
Next Review:	**June 2024**

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 students, the staff and the school and the Trust.

1.2. There will be school specific procedures which state whether personal mobile devices can be used within the school setting.

1.3. Pupils are responsible for using the school IT systems in accordance with this policy and the Pupil Acceptable Use Agreement which is an appendix to this policy (secondary age pupils only).

1.4. Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about e-safety campaigns and literature. Parents and carers will be responsible for endorsing the Pupil Acceptable Use Agreement, which is an appendix to this policy (Secondary age pupils only).

1.5. The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

1.6. The school will deal with such incidents within this policy and the behaviour management policy and will inform parents/carers of incidents of inappropriate e-safety behaviour. We do not have the resources to investigate all out of school incidents that take place on social media sites and recommend that pupils and parents/carers contact the social media site/the police in cases of inappropriate use/harassment etc. We also encourage the use of reporting via the CEOP reporting website https://www.ceop.police.uk/ceop-reporting/ and https://reportharmfulcontent.com/

2. E-Safety and Internet Use

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.

l. 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.

3. Designated Safeguarding Lead

The Designated Safeguarding Lead will:

a. take day to day responsibility for e-safety issues;
b. ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
c. provide training and advice for staff;
d. liaise with school ICT technical staff;
e. receive reports of e-safety incidents and create a log of incidents to inform future e-safety developments.

4. The Trust IT Team

The Trust IT Team will ensure:

a. that the school's ICT infrastructure is secure and is not open to misuse or malicious attack;
b. that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed;
c. that the use of the network is regularly monitored in order that any misuse can be reported to the E-Safety Co-ordinator for investigation and action where necessary;

d. that monitoring software systems are implemented and updated as agreed in school policies;

5. School staff

School 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 pupils are on a professional level and only carried out using official school systems;
e. pupils understand and follow this 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 pupils 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. The School's Designated Safeguarding Officer

The Designated Safeguarding Officer is trained in e-safety issues and is aware of the potential for serious Child Protection issues to arise from:

a. sharing of personal data;
b. access to illegal / inappropriate materials;
c. inappropriate on-line contact with adults / strangers;
d. potential or actual incidents of grooming;
e. cyber-bullying.

7. Education

7.1. Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

7.2. E-Safety education will be provided in the following ways:

a. a planned e-safety programme will be provided as part of the Computing and PSHE curriculum - this will cover both the use of ICT and new technologies in school and outside school;
b. key e-safety messages in assemblies and tutorial activities;

c. students will be taught in all lessons to be critically aware of the content they access on-line and will be guided to validate the accuracy of information.

8. Curriculum

8.1. e-safety is a focus in all areas of the curriculum and staff reinforce e-safety messages in the use of ICT across the curriculum;

8.2. where students are allowed to freely search the internet, staff are vigilant in monitoring the content of websites visited;

8.3. it is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager can temporarily remove those sites from the filtered list for the period of study. Any request to do so is audited with clear reasons for the need analysed and documented;

8.4. students are taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information.

9. Technical – infrastructure / equipment, filtering and monitoring

The school's IT systems are managed in ways that ensure that the school meets the e-safety technical requirements. There are regular reviews and audits of the safety and security of the school's IT system servers, wireless systems and cabling to ensure they are securely located and physical access is restricted.

a. all users have clearly defined access rights to school ICT systems
b. all users are provided with a username and password
c. the "master / administrator" passwords for the school IT system, used by the IT Management team, are available to the Chief Executive Office (CEO) and Deputy CEO, Head teacher and kept in a secure place
d. users will be made responsible for the security of their username and password. They must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
e. the Trust maintains and supports the managed filtering service
f. Trust IT technical staff regularly monitor and record the activity of users on the school IT systems
g. The school infrastructure and individual workstations are protected by up to date virus software
h. personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. Staff who need to do this in their particular role have should use an encrypted school device.

10 Unsuitable/Inappropriate Activities

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

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

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

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

f. 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.

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

11 Responding to Incidents of Misuse

11.1 Any apparent or actual misuse which appears to involve illegal activity, will be reported initially to the Designated Safeguarding Lead 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

11.2 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.

12 Protocol for Use of School Mobile Technology Devices.

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

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

12.2 When using your Trust mobile device:

a. Turn it off and put it in an appropriate carrying case when travelling;
b. Take care when connecting the network cable and seating the mobile device on a docking station as the connections can be easily damaged;
c. Keep all drinks and any other liquids away from your device. Any spillage on the device can result in data loss and expensive repairs;
d. Do not leave it in full view in any 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;
e. Never leave it unattended in public places even for a very short period of time;

13 Protocol for use of Personal Mobile Technology Devices

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

13.2 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.

13.3 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.

13.4 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.

13.5 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.

13.6 Pupils can:

a. have their personal mobile technology device confiscated if this or any other relevant school 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;

b. not take personal mobile technology devices into examinations. Pupils 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.

c. 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;

d. 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.

14 Following Copyright Laws

14.1 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.

14.2 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.

14.3 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.

14.4 Pupils must not make, transmit or store an electronic copy of copyright material.

15 Policy Circulation

15.1 This Policy will be published on the Trust's website.

15.2 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: 22.06.22

Appendix A - Pupil IT Acceptable Use Agreement

Users are responsible for their use of school computer systems. The current IT infrastructure is owned by the school 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 students, the staff and the school.

The school reserves the right to examine or delete any files held on its computer systems and to monitor use of the Internet, e-mail and other online communications. Access should only be made via an authorised account and password, which should not be made available to any other person.

Violations of these rules will result in withdrawal of access to ICT resources and additional action may be taken in line with the existing school behaviour and sanctions policy.

SECTION A: General

a. Pupils making use of the computers must do so in a way that does not harass, harm, offend or insult others.
b. Are expected to respect the work of all the people who use the computers.
c. Should not attempt to install or store software of any type on computers or intranet.
d. Must not use the computers for commercial purposes e.g. buying or selling goods.
e. must only access the Internet for study purposes or for school authorised/ supervised activities.
f. Must only use mobile phones in specific learning activities under the supervision of a member of staff
g. Must not take personal mobile technology devices into examinations
h. Must not use the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials that are unlawful, obscene, or abusive.
i. Are expected to respect the work, ownership and rights of people outside the school as well as other users in school.
j. Pupils will be allocated a school e-mail address. They should only e-mail people they know or who the teacher has approved. They must not give personal information such as their address or telephone number to those who they contact via e-mail.

SECTION B -Users of Trust mobile technology devices

a. Return the mobile device to the school when it is no longer required;
b. Only use official stores for installing mobile apps e.g. Microsoft store, Apple store, Google Play;

c. Do not change security settings or amending configuration files. This includes disabling passwords, pin codes and any installed security programs (e.g. Anti-Virus applications);
d. Notify the school in the event that the mobile device is lost or stolen.
e. Turn it off and put it in an appropriate carrying case when travelling;
f. Take care when connecting the network cable and seating the mobile device on a docking station as the connections can be easily damaged;
g. Keep all drinks and any other liquids away from your device. Any spillage on the device can result in data loss and expensive repairs;
h. Do not leave it in full view in any 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;
i. Never leave it unattended in public places even for a very short period of time;