

Digital Technology Policy

Introduction

At Fortismere we understand the responsibility to educate our students on digital safety issues. Schools hold personal data on students, staff and other people to help them conduct their day-to-day activities. Fortismere has published Privacy Notices on its website to explain how it processes any personal data that is held.

Everybody in our school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Student and parents/carers guidelines and responsibilities

Digital safety in the curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-Safety guidance to be given to students on a regular and meaningful basis.

- The school has a framework for teaching internet skills.
- The school provides opportunities within a range of curriculum areas to teach students about digital safety.
- Educating students about the online risks that they may encounter outside school is also done informally when opportunities arise and as part of the digital safety curriculum.
- Students are aware of the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying.

Managing internet use

The school provides students with supervised access to the internet (where reasonable). Students will also use web based learning resources and platforms to facilitate learning and curriculum delivery.

- Staff will preview any recommended sites before use.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents/carers recheck these sites and supervise this work. Parents/carers will be advised to supervise any further research.
- Students using personal devices are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility to install or maintain virus protection on personal systems.

Emails

All students and parents/carers are expected to adhere to the generally accepted rules of etiquette, particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication, or to arrange to meet anyone without specific permission.

- Students must immediately tell a parent/carer /teacher/trusted adult if they receive an offensive email.
- Students are allowed to use their own email address for sending work to teachers as requested.

Safe use of images - Taking and storing images and film

With the written consent of parents (on behalf of students), the school permits the appropriate taking of images of students with school equipment.

- Students are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of other students, or staff without advance permission from the Co-Headteachers/SLT.
- Students must have permission from the Head teacher/SLT before any image can be uploaded for publication.
- Images and films of students are stored on the school's IT network.

Publishing students' images and work

On admission to the school, parents/carers will be asked to give consent for the school to use their child's work/photos in the following ways:

- On the school website and Twitter account
- In the school prospectus and other printed/online publications that the school may produce for promotional purposes.

The consent form is considered valid for the entire period that the child attends this school unless the parent/carer notifies the school that there is a change in the child's circumstances where consent could be an issue, for example divorce, custody or safeguarding issues.

Parents/carers may withdraw consent, in writing, at any time.

- Students' full names will not be published alongside their images and vice versa. Email and postal addresses of students will not be published. Students' full names will not be published.
- Before posting student work or images on our website/Twitter, a check will be made to ensure that consent has been given.
- Only our Communications Officer or the Co-Headteachers have the authority to publish content to our website.

Personal mobile devices (including phones)

- Students in Year 7 to Year 11 are prohibited from bringing 'smart' phones to school (meaning an internet enabled device or a device with a camera). Phones must be switched off and carried in bags.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate messages between any members of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on the personal devices of any member of the school community.
- Students bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Social media

It is parents/carers' responsibility to ensure that they work within the law in relation to their child's use of social media

- Students are not permitted to access their social media accounts on school equipment while at school.
- All students are advised to be cautious about the information given by others on social networking websites, for example users not being who they say they are.
- Students are taught to avoid placing images of themselves on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Students are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, email address, specific hobbies/ interests)
- Students are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals
- Students are encouraged to be wary about publishing specific and detailed private thoughts and information online.

- Students are asked to report any incidents of cyberbullying to the school.

Incident reporting and misuse of inappropriate content

- Students are aware of the procedures for reporting accidental access to inappropriate content. The breach must be immediately reported to a member of staff.
- Deliberate access to inappropriate materials by any student will lead to an investigation by the Co-Headteachers/LA and could possibly lead to a permanent exclusion and involvement of police for very serious offences.

Parental involvement

- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school (*at the end of this document*).
- Parents/carers are required to make a decision as to whether they consent to images of their child and their work being taken and used in the public domain (e.g. school website)
- Parents/carers are expected to sign a Home School Agreement containing the following statement or similar:
 - We will support the school approach to on-line safety and not deliberately upload or add any text, image, sound or videos that could upset or offend any member of the school community.
- The school disseminates information to parents relating to digital safety through the School website and Newsletter items.

Guidelines to support parents when talking to their child about digital technologies

- Boundaries: There are age limits on certain technologies, make sure that you are aware.
- Parental controls: Adjust settings in line with your child's age and maturity.
- Social networking sites: Make yourself a friend so that you can monitor their activities.
- Remind your child that anything posted can be seen, copied, changed and forwarded to other people. Prospective employers may also look.
- Talk to them about information they have found, how it might be detrimental and how to protect their privacy.
- Discuss how they behave to others online, what they post online and inappropriate sites.
- Discuss downloading and plagiarism so they are aware of the legal implications.
- These website may be helpful:
 - <http://www.saferinternet.org.uk/advice-and-resources/young-people/11-19s>
 - http://www.thinkuknow.co.uk/14_plus/need-advice/selfies-and-sexting/

Fortismere Student Acceptable Use Agreement/Digital Technologies e-Safety Rules

- I will only use ICT systems in school, including the internet, email, digital video, and mobile technologies for school purposes.
- I will not download or install software on school technologies.
- I will only log on to the school network, systems and resources with my own user name and password.
- I will follow the school's ICT security system and not reveal my passwords to anyone.
- I will make sure that all ICT communications with students, teachers or others are responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to a teacher.
- I will not give out personal information such as name or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher.

- Images of students and/or staff will only be taken, stored and used for school purposes in line with school policy and not be distributed outside the school network without the permission of the Co-Headteachers.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, students or others distress or bring the school into disrepute.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/carer may be contacted.

Parents/Carers will be asked to read this policy and to discuss the policy and the Acceptable Use Agreement with their child as part of their admission to Fortismere

Policy date: March 2019