William Brookes School

The 3-18 Education Trust

E-Safety Policy

Member of Staff Responsible	CEO (statement of intent for trust), Headteacher for procedure and implementation of e-safety at school.
Relevant guidance/advice/legal reference	KCSiE (2021)
Adopted by	Individual schools and trust office
Date of Policy	January 2022
Review Cycle	3 years
Date of Next Review	January 2025

This policy is in two sections.

Section 1: this covers the trust-based intention for e safety and recognises the link with the Prevent duty, use of mobile phones and general cyber security.

Section 2: the school's and trust's implementation of the policy.

Section 1 (Trust)

Statement of Intent (from the Trust)

This policy is not a statutory requirement, but its existence recognises the significance of students and staff remaining safe whilst accessing resources online.

The 3-18 Education Trust has the highest regard for E-safety in its schools in order to promote safe and responsible use of technology. We are committed to using new technology to enhance the curriculum and educational opportunities whilst equipping our children and young people with the knowledge and understanding to stay safe and vigilant when online, both in school and outside.

E-safety involves the safe and responsible use of technology. This includes the use of the internet and also other means of communication using electronic media (e.g. text messages, email, gaming devices).

E-safety is not just about technology, it is also about people and their actions.

Technology provides unprecedented access to new educational opportunities through online collaboration, learning and communication. At the same time, it can provide the potential for staff and students to access material they should not access or it may lead to staff and students being treated by others inappropriately.

E-safety is part of the wider duty of care of all those who work in schools: equipping children and young people to stay safe online, both in school and outside and is integral to a school’s ICT curriculum. It may also be embedded in Personal Social and Health Education (PSHE) and Relationships, Sex and Health Education and include how staff and students should report incidents

Advice and resources on internet safety are available at: https://www.saferinternet.org.uk/
In association with the relevant Acceptable Use Policy Agreement (AUP), this policy forms part of the school’s commitment to educate and protect all users when accessing digital technologies, both within and outside school. It should be read in conjunction with other relevant policies, such as the Child Protection and Behaviour policies.

The Education and Inspections Act 2006 empowers headteachers to such extent as is reasonable to regulate the behaviour of students when they are off the school site and (the Act) empowers members of staff to impose sanctions for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other online safety incidents covered by this policy, which may take place outside of the school but which are linked to membership of the school.

Schools will, where it becomes known, inform parents/carers of any such incidents of inappropriate online behaviour that takes place out of school.

The 2011 Education Act increased these powers with regard to the searching for electronic devices and the examination of any files or data (even where deleted), on such devices.

The Prevent Duty (See Preventing Radicalisation and Extremism Policy)

As organisations seek to influence young people through the use of social media and the internet, schools and childcare providers need to be aware of the increased risk of online radicalisation and the risks posed by the online activity of extremist and terrorist groups.

The Prevent duty is the duty under the Counter-Terrorism and Security Act 2015 on specified authorities (schools and childcare providers), in the exercise of their functions, to have due regard for the need to prevent people from being drawn into terrorism. The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools.

The Prevent duty means that all staff have a duty to be vigilant, and where necessary, will report concerns about internet use that includes, for example, the following:

- Internet searches for terms related to extremism
- Visits to extremist websites
- Use of social media to read or post extremist material
- Grooming of individuals

https://www.educateagainsthate.com/

The use of devices in school, which are not owned by school

Mobile phones: If a student wishes to bring these into school, they must be switched off and put away (kept out of sight). The trust recognises the value that a mobile phone can have at the start and finish of the school day, but also the significant distraction and potential harm that the use of a mobile phone can bring when used in school.

Students found to be in breach of this requirement will have their device confiscated. These can be collected at the end of the day. If a member of staff suspects that a mobile phone has been misused within the school, then it should be confiscated and the matter dealt with in line with normal school procedure (see below).

Cyber bullying

All forms of bullying (including cyberbullying) should be handled as a community issue for the whole school. Every school has measures in place to prevent all forms of bullying. These measures should be part of the school's behaviour policy which are communicated to all pupils, school staff, governors and parents.

Cyber bullying is defined as '*the use of modern communication technologies to embarrass, humiliate, threaten or intimidate an individual in the attempt to gain power and control over them*.'

Cyber bullying against staff

The DfE state that '*all employers, including employers of school staff in all settings, have statutory and common law duties to look after the physical and mental health of their employees. This includes seeking to protect staff from cyberbullying by pupils, parents and other members of staff, and supporting them if it happens*'.

Cyberbullying: Advice for headteachers and school staff is non-statutory advice from the Department for Education for headteachers and all school staff on how to protect themselves from cyberbullying and how to tackle it if it happens.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Section 2: School-based implementation and policy

Individual schools are responsible for their E-Safety procedures and are given freedom to manage their provision. This is due to their different contexts with respect to key stages. Day to day responsibility for educating pupils in E-safety settings lies with the headteachers and other staff with responsibility for the IT provision in schools.

The E-safety policy applies to all members of the school community, including staff, governors, pupils, volunteers, parents, carers, and visitors. This includes anyone who uses and/or has access to, personal devices and technologies whilst on school site and those who have access to, and are users of, school devices and technologies, both in and outside of the school.

Purpose

The purpose of this statement is to outline how the school will deliver safe and responsible use of ICT throughout school and give clear guidelines (Acceptable Use Agreements) to staff, pupils and volunteers.

Roles and responsibilities

Acceptable use policies (and breaches) – Staff, students

Use of devices (passwords, data storage (data protection) emails, phones, photographs)

Process of reporting

Training