Tomlinscote School & Sixth Form College

A Specialist Language College

E-Safety Policy (Staff)

Policy Type:	Mandatory
Approved By:	Resource Committee
Effective From:	May 2018
Revision Date:	May 2021

Tomlinscote School
e-Safety Policy

We believe that ICT has a critical role in equipping students for life in the 21st Century and that ICT can have a positive impact on teaching and learning. To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom. This policy document has been drawn up to protect all parties – the students, the staff and the school, and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

Our e-safety and policy has been written using British Educational Communications and Technology Agency (BECTA) guidance.

1. Staff Responsibilities

All staff are responsible for promoting and supporting safe behaviours in their classrooms and for following e-Safety procedures. Staff should also be aware of their personal responsibilities to protect the security and confidentiality of the school network.

1a. To safeguard the welfare of children

The *Children Act 2004*[1] and the policy document *Working Together to Safeguard Children*[2] sets out how organisations and individuals should work together to safeguard and promote the welfare of children.

The 'staying safe' outcome includes aims that children and young people are:

- Safe from maltreatment, neglect, violence and sexual exploitation;
- Safe from accidental injury and death;
- Safe from bullying and discrimination;
- Safe from crime and anti-social behaviour in and out of school and;
- Secure, stable and cared for.

These aims apply equally to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms. For example, there is a need to protect students from dangers such as:

- The use of the internet for grooming children and young people with the ultimate aim of sexual exploitation;
- The use of ICT as a new weapon for bullies, who may torment their victims via websites or text messages and;

- Exposure to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour.

It is the duty of all staff to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

1b. To ensure security and confidentiality

- Maintain password security. Passwords should not be shared with any other member of the school community, nor should they be written down;
- Staff IT devices must also be password-protected;
- When unattended, IT devices must be logged off or locked down. This is equally applicable in classrooms, departmental areas and in offices;
- All computers and associated equipment must be shut down and turned off at the end of the day;
- Data storage devices such as USB pens, portable hard drives, CD-Roms and DVD-Roms must be subject to virus protection measures by 'stopping' devices before removal from the computer, and not inserted in the first instance if the source cannot be trusted;
- Any accidental access of inappropriate material on the internet should be reported to the e-Safety Coordinator immediately (RM: Head of School). The school reserves the right to examine internet access logs from any computer in the school and staff laptops issued by the school. Neither the school nor the Academy Trust can accept liability for material accessed, or any consequences of Internet access;
- E-mails from suspicious sources should not be opened. These should be reported to the network manager. Software should not be downloaded unless the source can be trusted and the member of staff has checked that there is no infringement of licensing laws and;
- Photographs of students should only be taken and saved on the network where permission to do so has been freely given by parents or the student themselves.

1 c. To safeguard the facilities and support student behaviour

Vigilance by staff in supervising and monitoring student use of ICT will reduce the incidence of damage to expensive resources and help to secure e-Safety for the students. The expectations of students are clearly described in the 'ICT Student Agreement.' Expectations of staff are described below:

- Students must always be supervised in ICT suites and in classrooms where laptops are in use. The doors should be locked in the absence of a member of staff;
- Upon discovery, all damage must be reported immediately;
- Seating plans must be used to ensure that any subsequent damage can be tracked to individual students;

- Ceiling projectors must be turned off when they are not in use by using the remote control;
- Food and drink must not be consumed in ICT suites or in classrooms where laptops are in use;
- Portable laptops used in lessons must be returned to the trolley and locked after use by a class and;
- Students should not be given access to electrical equipment if they have wet clothing.

2. How will complaints regarding e-Safety be handled?

The school will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- Interview, counselling and/or disciplinary action by tutor, Head of Year, e-Safety Coordinator, Child Protection Officers, Head of School or the Interim Principal;
- Informing parents or carers;
- Removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework];
- Referral to the Local Authority / Police.

Our e-Safety Coordinator will act as first point of contact for any complaint. Any complaint about staff misuse will be referred to the Head of School and may result in formal disciplinary proceedings.

Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school child protection procedures.

I understand my responsibilities as described in this e-safety policy:

Signed: …… (Staff)

Print Name…….

Date ……

1. *See The Children Act 2004 [http://www.opsi.gov.uk/acts/acts2004/20040031.htm]*
2. *Full title: Working Together to Safeguard Children: A guide to inter-agency working to safeguard and promote the welfare of children.*