

# Merchant Taylors' School

---

## E-SAFETY POLICY

**Policy Custodian:** Senior Master

**Approving Body:** MTS Senior Leadership Team

**Approved:** September 2023

*(This policy does not apply to Merchant Taylors' Prep.)*

### Contents

#### 1. Introduction and Overview

- Rationale and Scope
- Roles and responsibilities
- How the policy be communicated to staff/pupils/ School community
- Handling complaints
- Review and Monitoring

#### 2. Expected Conduct and Incident Management

#### 3. Managing the ICT Infrastructure

- Internet access, security (virus protection) and filtering
- Network management (user access, backup, curriculum and admin)
- Passwords policy
- E-mail
-

## 1. Introduction and Overview

### **Rationale. The purpose of this policy is to:**

- set out the key principles expected of all members of the school community at Merchant Taylors' School with respect to the use of ICT-based technologies and connectivity.
- safeguard and protect the pupils and staff of Merchant Taylors' School
- assist school staff working with pupils to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- have clear structures to deal with online abuse such as cyberbullying.
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- minimise the risk of misplaced or malicious allegations made against adults who work with pupils.
- promote digital literacy and help foster a positive online environment.

### **The main areas of risk for Merchant Taylors' can be summarised as follows:**

#### **Content**

- exposure to inappropriate content, including but not limited to online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- lifestyle websites, for example self-harm/suicide sites
- hate sites
- content validation: how to check authenticity and accuracy of online content

#### **Contact**

- grooming
- cyber-bullying in all forms
- identity theft (including 'fraping' (hacking Facebook profiles)) and sharing passwords
- radicalisation

#### **Conduct**

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (Internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- copyright (little care or consideration for intellectual property and ownership – such as music and film, still and video imagery)

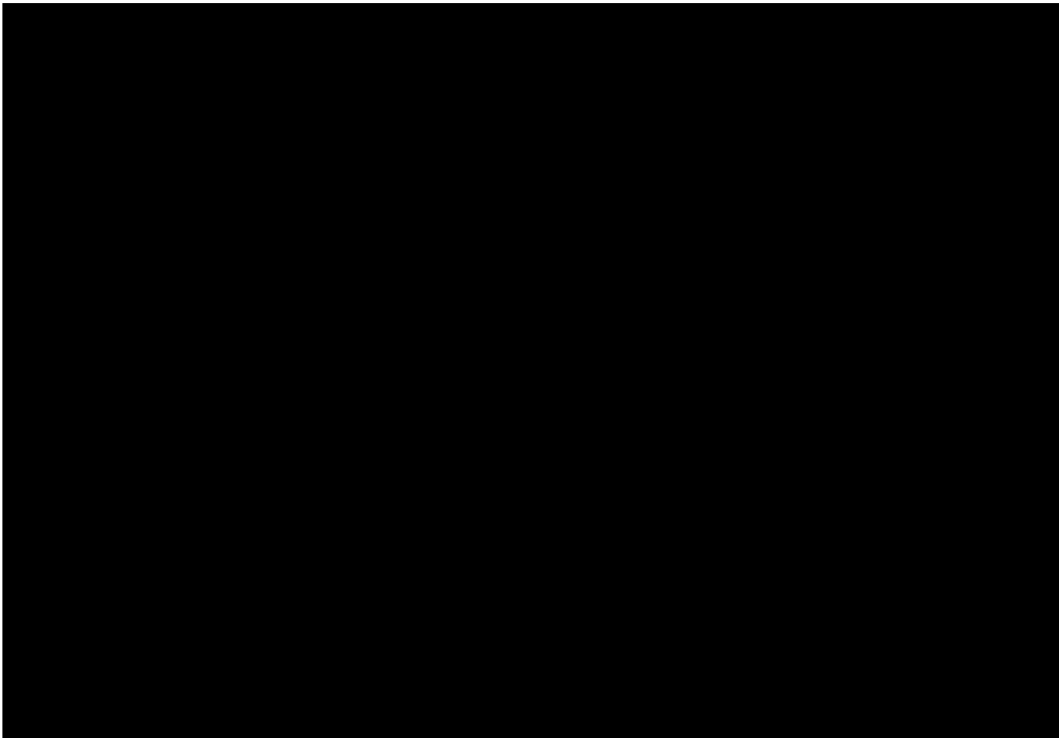
#### **Scope**

This policy applies to all members of Merchant Taylors' School community (including staff, pupils, volunteers, parents / carers, visitors) who have access to and are users of School ICT systems and connectivity, both within and outside of the grounds of Merchant Taylors'.

The Education and Inspections Act 2006 empowers the Head Master 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. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers

with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Good Promoting Behaviour Policy.

Merchant Taylors' will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

<b>Role</b>	<b>Key Responsibilities</b>
Head Master	To take overall responsibility for e-safety provision; To take overall responsibility for data and data security; To ensure the school uses an approved, filtered Internet Service; To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant; To be aware of procedures to be followed in the event of a serious e-safety incident; To receive monitoring reports as required from the Senior Master; To ensure that there is a system in place to monitor support staff who carry out internal e-safety procedures.
Senior Master	



## Pupils

Read, understand, sign and adhere to the Pupil Acceptable Use Agreement have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulation;

To understand the importance of reporting abuse, misuse or access to inappropriate materials;

To know what action to take if they or someone they know feels worried or vulnerable when using online technology;

to know and understand school policy on the use of smartphones, digital cameras and hand held devices including tablets which are used by boys from year 9 upwards;

To know and understand school policy on the taking / use of images and on cyber-bullying;

To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-

## **Review and Monitoring**

The e-safety policy should be read in conjunction with school policies: Acceptable use of ICT Policy, Child Protection Policy, Anti-Bullying Policy, the School Development Plan, Promoting Good Behaviour Policy, Personal, Social and Health Education Policies.

- The e-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- The e-safety policy has been written by the

### 3. Managing the ICT infrastructure

#### Internet access, security (virus protection) and filtering

This school:

Has secure broadband connectivity supplied by British Telecom, a national provider of Internet in education;

Uses a [Fortinet filtering system](#) which blocks sites that fall into content and web search categories including but not limited to:

- **Illegal:** content that is illegal, for example child abuse images and terrorist content
- **Bullying:**





Does not allow any outside Agency to access our network remotely except where tk

**Password policy**

This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it;

All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private;

We require users to create a password that is a minimum of 14 characters long and they must contain three of the four categories of uppercase, lowercase, numerical characters and symbols e.g. QuickBlackHorse23! would fit all requirements;

We require pupils and staff to change their network passwords at least termly.

Users cannot use any of the last three passwords.

**E-mail**

This school:

Provides staff with an email account for their professional use, and makes clear that personal email should be through a separate account;

Does not publish personal e-mail addresses of pupils on the school website;

Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law;

The Head Master takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;

Staff are very