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.
- Outline the technological measures in place to comply the filtering and monitoring obligations first outlined in KCSIE, September 2024.

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

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.

Role	**Key Responsibilities**
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	Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents; Promotes an awareness and commitment to e-safeguarding throughout the school community; Ensures that e-safety education is embedded across the curriculum and liaises with school ICT technical staff; To communicate regularly with DSL and Director of Digital Strategy as required to discuss current issues, maintain monitoring and and internet filtering logs; To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident; Facilitates training and advice for all staff; Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: sharing of personal data access to illegal / inappropriate materials inappropriate on-line contact with adults / strangers potential or actual incidents of grooming cyber-bullying and use of social media
Head of Computing	To oversee the delivery of the e-safety element of the Computing curriculum; To liaise with the Director of Digital Strategy regularly
IT Manager	To report any e-safety related issues that arises, to the Senior Master; To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed; To ensure that provision exists for misuse detection and malicious attack e.g. keeping anti-virus protection up to date; To ensure the security of the school ICT systems; To ensure that access controls exist to protect personal and sensitive information held on school-owned devices;

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

- Complaints of cyberbullying 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.

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, 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 Senior Master and is kept up to in line with technical advances so it is appropriate for its intended audience and purpose.

2. Expected Conduct and Incident management

Expected conduct

In this school, all users:

are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems;

need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences;

need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;

should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school;

Staff

are responsible for reading the school's e-safety policy and using the school ICT systems accordingly, including the use of smartphones, and hand-held devices including touch-screen tablets issued to staff.

Pupils

should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. Pupils also need instructions to appropriate and inappropriate use of AI systems such as Chat GPT or Microsoft Co-pilot

Parents/Carers

should provide consent for pupils to use the Internet, as well as other technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the school;

should be aware that the School may impose sanctions from misuse of ICT Systems.

Incident Management

In this school:

there is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions; the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions;

all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes;

support is actively sought from other agencies as needed;

monitoring and reporting of e-safety incidents takes place and contribute to developments in policy and practice in e-safety within the school. The records are reviewed/audited and reported to the school's senior leaders;

parents are specifically informed of serious e-safety incidents involving young people for whom they are responsible;

Uses ‘remote’ management control tools for controlling workstations / monitoring user activity / setting-up applications and Internet web sites, where useful;
Storage of all data within the school will conform to the UK data protection requirements
Pupils and Staff using mobile technology, where storage of data is online, will conform to guidance issued from HM Government.

As MTS has adopted digital learning via 1:1 scheme centred on Surface tablets, SENSO monitoring software has been installed on student touch screen devices to allow for teacher

Ensures staff

E-mail

This school:

Provides staff with an email account for their professional use, and makes clear that personal email use should largely 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;

Will ensure that email accounts are maintained and up to date;

Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police;

Knows that spam, phishing and virus attachments can make e-mails dangerous. We use a number of cyber security technologies to help protect users and systems in the school, including Barracuda Total Email Protection, Watchguard AD360 EDR, Fortigate web filtering, plus direct Microsoft email filters. These are designed to block malware including viruses, Trojans, pornography, phishing and inappropriate language.

(Barracuda has been a member of the Internet Watchfoundation since 2009)

(Microsoft

Learning platform

Uploading of information on the schools' Teams and SharePoint system is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas

We do not identify pupils full names of pupils in the credits of any published school-produced