



**eSafety Policy**  
to be amalgamated in  
**Online Safety and IT Acceptable Use Policy**  
(currently in draft format)

<b>Title of Policy</b>	eSafety Policy
<b>Applies to</b>	Whole School: Staff and Volunteers
<b>Endorsed by</b>	Head Master
<b>Responsibility</b>	Deputy Head (Pastoral)
<b>Date reviewed</b>	Michaelmas Term 2023
<b>Next review</b>	Michaelmas Term 2024

## Introduction

The School encourages pupils to use new technologies for their important educational and social benefits. This policy aims to balance the desirability of fully exploiting this potential with providing safeguards against risks and unacceptable materials and activities. The policy covers both technologies provided by the School and those owned by pupils and staff but brought onto the school premises. Although pupils may be trusted by their parents with regard to private internet use, the school has a legal obligation to safeguard all pupils.

The Deputy Head (Pastoral) is the School's eSafety coordinator and the DSL. eSafety and Safeguarding issues are dealt with by the Safeguarding team, in line with the School's [Child Protection and Safeguarding Policy](#).

Concerns regarding cyberbullying can be reported to any member of staff, in accordance with the [Anti-Bullying Policy](#) and should then be reported to the Deputy Head (Pastoral) and DSL for necessary action in line with the [Behaviour Management Policy](#) and the [IT-Related Sanctions Policy](#).

## Issues

Pupils are keen to grasp the opportunities offered by new technology and the availability, portability, miniaturisation and sophistication of electronic devices. However there are associated risks which include the following: exposure to inappropriate material, physical danger, cyber-bullying, legal and commercial issues, gambling and addictive behaviour.

## Aims

The School aims to protect and safeguard pupils in their use of technology by:

- Ensuring that all pupils are IT literate and can use the facilities so that their education provision is enhanced to the maximum.
- Raising awareness and countering instances of cyber-bullying. Cyber-bullying is when the Internet, mobile phones or other devices are used to send or post text or images intended to hurt or embarrass another person. It may also include threats, sexual remarks, pejorative labels (i.e. hate speech), ganging up on victims by making them the subject of ridicule in forums, and posting false statements as fact aimed at humiliation. (See also [Anti-Bullying Policy](#) and [Social Networking Policy](#)).
- Raising awareness and building resilience to radicalisation, through PSHE sessions and communication with parents, in combination with filtered internet access.
- Enabling appropriate and careful use of social networking sites or personal web pages.

## Procedures and Practices

The School provides every pupil with internet access and access to the School's own network. The following measures are in place to protect the safety and interests of all pupils and staff and inhibit abuses:

**The Use of Technology** – The School operates a [Bring Your Own Device](#) policy, ensuring that all

pupils have access to a laptop, chromebook or similar device in lessons, when the teacher decides their use is beneficial to the lesson objectives. Visitors to the site may be given a time-limited code, providing access to a restricted wifi network, where necessary. All visitors are subject to the terms of the [Visitors' Policy](#).

**Mobile Phone Use within School ([Mobile Phone Poster](#))**- pupils are not required to have mobile phones in School. We ensure that all internal communication necessary can take place within school without the need for a mobile phone device. Currently no pupil in Year 6 and below is allowed a mobile device in School. If a pupil in Year 7 or above needs to bring their phone into School, the following expectations apply:

**Years 7-9: mobile phone handed in to Houses during the school day.** All Houses have a secure locker to store phones. For functional reasons only, pupils can use their mobile phones within a designated area of their House, but only under the discretion of house staff. Exceptions for late drop off (e.g. after an ensemble) or early collection (e.g. for fixtures) can be arranged with house staff.

**Years 10-11 (and Year 9 on Saturday mornings): mobile phone 'hidden' during the school day** (Phones off, away in bags and out of sight). For functional reasons only, pupils can use their mobile phones within a designated area of their House, but only under the discretion of house staff.

**Sixth Form: mobile phone 'hidden' during the school day** (Phones off, away in bags and out of sight). For functional reasons only, pupils can use their mobile phones within the Sixth Form Centre or Ritchie House.

**Exceptions:** for pupils requiring mobile phones for exceptional purposes, applications can be made to the Deputy Head (Pastoral) and a mobile phone 'pass' will be issued. The Head of SEND will maintain a list of pupils with permission to use a mobile phone due to particular needs along with the reason for it. This should be reviewed annually.

**Sanctions:** If a pupil is found using a mobile phone around the school site, it will need to be turned off and handed in to Reception. It can be collected at the end of the School day. Sanctions will be given in line with the School's [Behaviour Management Policy](#) and will typically be a Warning issued on iSAMS.

**Device Boundaries for Boarders** - all houses have a lockable electronic device locker for safe keeping of devices when needed. We encourage healthy use and management of devices in Houses to encourage good habits for life.

**Prep Time** - Boarders in Year 11 and below, hand in their mobile phones during prep time. Laptops can be used for study purposes only. For all pupils, Housestaff reserved the right to confiscate any device if it is being used inappropriately.

**Overnight** - Boarders in Year 11 and below hand in their electronic devices at night. Access to the wireless network is also limited overnight. The timings of wifi availability are decided in consultation with houseparents.

**IT Acceptable Use Policies for Staff and Pupils** - These protect all parties by clearly stating what is

acceptable and what is not, with regard to the use of technology in the classroom and beyond.

**Use of Usernames and Passwords** - All users, other than those in the Pre-Prep have their own private username and password. Pre-Prep pupils use generic accounts under close supervision from staff. All other pupils are advised not to be careless or negligent with their passwords. All network activity is logged.

**Building Resilience** - The School builds resilience in pupils to protect themselves and their peers from cyber bullying and other safeguarding issues under the banner of Digital Citizenship. This takes the form of assemblies and other Digital Citizenship sessions run for individual year groups, for example as part of pupil's induction at the beginning of the year. Further sessions in PSHE and assemblies address cyber-bullying, radicalisation and safe use of the internet, as well as talks from external speakers such as Dr Susie Davies. This is complemented by sessions run for parents, as part of the Parental Engagement Programme.

**Staff Training** - Staff are trained, as part of their professional development, in online safety and Digital Citizenship issues.

**Web filtering** - The School subscribes to a web filtering service that maintains a database which categorises websites and restricts access. In line with requirements, material that is classified as discrimination, drugs/substance misuse, extremism, malware/hacking, pornography, piracy and copyright theft, self harm and violence and hate are blocked by our filtering system. This is in line with the UK Safer Internet Centre's [Appropriate Filtering for Schools](#) guidance.

**Monitoring** - The School exercises the right to monitor the use of computer systems including monitoring of internet use, interception of emails and the deletion of inappropriate materials at all times. The school's filtering and monitoring systems block inappropriate content, monitor the use of the network by individuals and alert the school to potential safeguarding issues. This is in line with the UK Safer Internet Centre's [Appropriate Monitoring for Schools](#) guidance.

**Advice** - The Head of PSHE visits boarding houses from time to time when and if necessary, to discuss particular issues which have been raised by pupils. Concerns about e-safety are openly discussed in the house context and there is a culture of awareness.

**Parental Engagement** - The School runs regular sessions for parents/carers covering online safety and Digital Citizenship, as part of the Parental Engagement Programme. The purpose of these sessions is to create a shared understanding between staff, pupils and parents with regard to eSafety issues. Resources are available on the school intranet and are also sent to parents by email, highlighting key issues in cyberbullying, eSafety and use of social media.

**Management of Data** - The personal data of staff, students and parents is held and processed by the school, in accordance with statutory requirements and in line with the school's Data Protection Policy.

## **Expectations of Pupils and Parents beyond the School**

The School expects the use of technology by its pupils, even when at home, to comply with the School's stated ethos and to honour the agreement permitting the use of IT at school. Material downloaded in the home, posted on the internet using a home computer or transmitted to a mobile phone when a pupil is not at school, can impact significantly upon the lives of pupils and other

members of the School community. Pupils should be aware that computer/mobile phone, emails and social network sites may be scrutinised for the purposes of safeguarding or promoting a child's welfare or maintaining and promoting the wellbeing of the school community as a whole, in accordance with the School's [Social Networking Policy](#). Parents are strongly encouraged to help their children develop good habits of technology use at home through the Digital Citizenship programme.

## **Sanctions**

In the event of any breach of this policy the School will apply sanctions proportionate to the offence committed, in line with the School's [IT-Related Sanctions Policy](#) and the [Behaviour Management Policy](#). This may involve the advice and/or intervention of external agencies as necessary including the local police and Somerset safeguarding services.