IT, INTERNET, AND E-SAFETY POLICY

Rooted in Christ and Catholic tradition and under the guidance of its patron, St Edmund's aims to realise the God-given potential, in body, mind and spirit, of all members of its community through service and leadership.

Avita Pro Fide

St Edmund's is committed to ensuring the welfare and protection of children in their care and this commitment is a fundamental part of the role of every employee.

This policy covers all devices in the College which are connected to the College network.

The College will encourage and enable each student to use IT to enhance their learning and to give them the skills that they will need in a society that relies heavily on technology.

The College will achieve this by:

- maintaining and enhancing the provision of technology for students through a planned investment in hardware, software, and staffing. Thus, it will ensure appropriate levels of access to IT equipment for all students.
- looking at the strategic development of IT throughout the College through the work of an IT steering committee; and IT Co-ordinator
- delegating to Heads of Department the role of using IT within their schemes of work.
- providing appropriate training for staff to develop their skills in using IT in their teaching.
- providing rules and guidance to all staff and students concerning the use of IT to access the world outside the College.
- educating all members of the community in e-safety: students through the PSHE programme, staff through briefings and parents through presentations at parent meetings

The College will also:

1. Ensure that IT is used efficiently to help teaching staff in the administrative aspects of their work.
2. Set guidelines to help to ensure that its staff and students work within the law as set out by the Data Protection Act and GDPR.
3. Employ filtering/firewall systems to minimise the possibility of staff, students and visitors accessing inappropriate material, including websites with inappropriate content.
4. Ensure that serious and/or repeated breaches or attempted breaches are reported, as appropriate under the College disciplinary procedures, including to Child Protection agencies and Police where necessary.
5. Ensure compliance with regulatory policies and procedures, including the Prevent Duty.

What St Edmund's College is doing to provide protection:

St Edmund's College has a range of security software and hardware at its disposal which is constantly upgraded and enhanced. These include:

CCTV – The College uses CCTV systems that monitor student activity 24 hours a day every day, at multiple points around the campus. This footage is frequently reviewed during and after any incident which might occur to ensure the safety and security of both the students and the IT systems.

Network Security Software – The entire computer network is secured by a range of software solutions designed to provide protection for its users.

Filtering Systems - Internet filtering and logging software provides security for all students by actively blocking web sites containing material which St Edmund's College deems as inappropriate. This system logs all the students' internet activity allowing the IT Technical Staff to produce reports broken down to a particular moment of the day.

Email filtering and logging software is installed on our email server scanning all incoming and outgoing emails for computer viruses, spam, bad language and inappropriate attachments.

Frequency of review: 3 years
Policy last reviewed: Michaelmas 2021
Next review date: Michaelmas 2024

Appendix 1

Acceptable Use Policy for Students

The use of the College's IT resources and services is a facility granted, at the College's discretion, to students. This Acceptable Use Policy is designed to ensure appropriate use of devices and the College's networks as well as ensuring students can benefit from using the College systems.

Use of the College network constitutes agreement to comply with this policy.

These rules apply to a student's use of the College network, whether using College computers or devices or using their own devices as a method to log in. This also applies to accessing the College network off site.

Students are given a user account to enable them to use the network and by continuing to use the network, users must abide by the following: -

Student Terms of Use

- You are responsible for account access on the College network. Any unauthorised use of your account should be flagged to the College's IT team immediately.

- Use of the College network is regularly monitored by the College's IT team (which includes email access). The College will monitor any traffic over the College system to prevent threats to the College's network.

- You must not use someone else's username to gain access to the College network.

- You must not share your password with anyone else.

- You are not permitted to share access details to the College's network or Wi-Fi password with anyone else.

- You must not attempt to circumvent security of any host, network, or account, or penetrate security measures ("hacking") on or accessed through the College network.

- You must not probe, scan, or test the vulnerability of the network or other networks.

- You must not try to install any software on College systems.

- Any apps or software that are downloaded onto your personal device whilst using the College's network is done at your own risk and not with the approval of the College.

- You must not use the network or your own property to access or process inappropriate materials. This includes (but is not limited to) pornographic material, material which may be

seen as violent, offensive, or discriminatory, inappropriate text files, or files dangerous to the integrity of the network.

- You must not transmit, re-transmit, publish, or store material or messages on or through the College network which could be perceived as bullying, threatening, abusive, hateful, indecent, harassing, offensive or defamatory.

- You must report any inappropriate messages or information immediately to the IT team. This report will help protect other pupils and you.

- You must not record, video, or take pictures of other students, staff or third parties without express permission.

- Eating and drinking are not suitable activities in any classroom. Near a computer these may cause serious damage and are strictly prohibited.

- Use of own devices is at the risk of the user. The College cannot accept responsibility for any loss, damage or costs incurred due to use, damage or loss whilst accessing the College's systems.

- Storage media, such as USB sticks and hard drives, are prohibited in the College.

- Any property owned by students, such as mobile phones and iPads, may not be used to stream, download, or watch videos.

- You may not access the internet except through the College network

- Computer (file) storage areas will be treated as school property. IT staff may look at files and communications to ensure that the system is being used responsibly. Users should not expect that their work and emails would always be private.

- Above all, you should be KIND ONLINE

- Intentional damage to computers, computer systems or computer networks, including unauthorised damage or interference to any files is not permitted and may be considered a criminal offence under the Computer Misuse Act.

- The College BYOD setup may install software to aid in internet filtering. This is a security requirement for most networks and is only used when inside the College. Please be aware of this before connecting your computer to the College wireless network and seek clarification from the IT department if you have any questions.

If a student or user account breaches the above rules, their account may be inspected, and their access stopped. A breach may also be sanctioned in accordance with the College's Behaviour Policy.