St Edmund's College & Prep School

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 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 metings

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.
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.

Frequency of review: 3 years
Policy last reviewed: Michaelmas 2018
Next review date: Michaelmas 2021

IT USAGE – The College Network for Students

Access to the school network is provided for recognised schoolwork only and on the understanding that users agree to observe the following guidelines which apply to both pupils and staff.

Computer (file) storage areas are treated as school property. IT staff are expected to monitor use and may look at files and communications to ensure that the system is being used responsibly at all times. Users must accept that their work and emails are not private. The system allows IT staff access to view any computer screen at any time from anywhere on the school network without a user being aware of it.

- Users are responsible for good behaviour on the network just as they are in a classroom or a school corridor. General school rules apply.
- Eating, drinking, and the use of aerosol sprays are not suitable activities in any classroom. Near a computer these may cause serious damage and are strictly prohibited.
- If a "virus alert" occurs when transferring work files from a USB Memory Stick a member of the IT staff must be informed immediately.
- The use of another person's password is forbidden. When doing shared work, duplicate copies must be kept of the work on each user's storage in case the partner is absent from school.
- A user's password must not be revealed to anyone else. If a user thinks that someone has learned their password, it should be changed immediately by seeing members of the IT staff.
- Access to the folders, work or files of another user is forbidden.
- The unauthorised access or use of personal information, contrary to the provisions of the Data Protection Act, is not permitted.
- 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
- Programs must not be installed on a computer except by a qualified technician. Do not bring in programs on a USB Memory Stick or download these from the Internet.
- Games must not be loaded, played or used on any computer unless used for authorised training or teaching purposes.
- The unauthorised copying of software, contrary to the provisions of the Copyright, Designs & Patents Act , is not permitted.
- The installing, copying or transmitting of obscene material is not permitted and may be considered a criminal offence under the Obscene Publications Act
- Computer equipment should not be taken off-site without formal authorisation.
- Users should always make sure that they have completely logged off the computer before leaving it unattended.
- The computer and the surroundings should be left as they were found.

Sanctions

1. Violations of the above rules will result in the user receiving a temporary or permanent ban on the use of the school network.
2. Additional disciplinary action may be added in line with existing practice on inappropriate language, bullying or other behaviour.

IT USAGE – Use of the Internet for Students

Internet access will be provided to conduct research and communicate with others, but only on the understanding that the following guidelines, which apply to both pupils and staff, are agreed and accepted.

General

- Users are responsible for good behaviour on the Internet just as they are in a classroom or a school corridor. General school rules apply.
- The Internet is provided for users to conduct genuine research and communicate with others. All the sites users visit are recorded. Remember that access is a privilege, not a right and that access requires responsibility at all times.
- 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.
- Users should be aware that a member of the IT staff can view their computer screen at any time from anywhere on the school network without their knowledge.
- During lessons, teachers will guide pupils toward appropriate materials. Outside of lessons, families bear responsibility for such guidance, as they must also exercise with information sources such as television, telephone, cinema, radio, newspaper, magazine and other potentially offensive media.

The following are Not Permitted:

- Sending, displaying, accessing or trying to access any obscene or offensive material.
- Accessing sites which include the following material:
    - Pornography
    - Racism and other forms of discrimination
    - Radicalisation
    - Extremism
    - Intolerance of others' individual liberty
- Using obscene or offensive language. (*Remember that you are a representative of your school on a global public system - never swear, use vulgarities, or any other inappropriate language. Bad spelling is also a poor reflection on you and on the school.*)
- Harassing, insulting or attacking others through electronic media.
- Violating copyright laws. (*Never copy and make use of any material without giving credit to the author. By itself such work will be of little value as your own work.*)
- Revealing any personal information, the home address or personal phone numbers of you or other people.
- Downloading games or other executable programs.
- Intentionally wasting limited resources on unnecessary or unauthorised activities.

- Private use of the Internet or email service without advanced permission.
- Use of commercial activities by for-profit institutions.
- Carrying on a private business.
- Undertaking financial transactions on behalf of the school.

Check with a Member of the IT Department Before:

- Opening unidentified email attachments.
- Completing non College questionnaires or subscription forms.

Sanctions

Violations of the above rules may result in a temporary or permanent ban on Internet use. Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour.

Appendix 1 – **St Edmund's College IT Acceptable Use Policy (AUP)**

St Edmund's College IT Acceptable Use Policy (AUP)

Introduction

While no technological solution can be 100 per cent effective in guaranteeing safety when using the internet and related technologies, technology can help to minimise the risks to pupils, particularly when rules are in place to ensure protection. St Edmund's College is doing everything it can to provide a safe and enjoyable experience to all its students and for this to happen we require the support of all students and their parents/guardians.

To this end an Acceptable Use Policy has been created to inform students and parents about what St Edmund's College is doing to protect its users and to spell out a code of conduct which must be adhered to.

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 – All IT rooms and the Rhetoric King Room have digital CCTV systems in operation which monitor student activity 24 hours a day every day. 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. Within this we have a piece of software called NetSupport School which enables real time monitoring of student activities. Everything a student sees on their computer screen is duplicated on a teacher's screen and can even be recorded if a student is carrying out any activity which breaches this AUP.

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 is called iboss and is used in hundreds of schools around the country. iboss also 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 supplied through Barracuda and is installed on our email server scanning all incoming and outgoing emails for computer viruses, spam, bad language and inappropriate attachments.

St Edmund's College IT Code of Conduct

Use of the Internet and Email

- You must not use the Internet for personal use during lesson times.
- You must not knowingly try to access inappropriate sites, including those relating to violence, racism, drugs, bad language, pornography, extremism at any time.
- Do not try to access prohibited websites or attempt to bypass the College security and filtering systems.
- Do not give personal addresses, telephone numbers or email addresses belonging to you, any other student or member of staff over the internet.
- Do not download any material which is copyright including music and video files. Always seek permission from the owner before using any material from the Internet.
- Do not send offensive emails to other students, members of staff or anyone outside the College. This includes foul language and messages which could be deemed as bullying.
- Should a student gain access to an inappropriate site then they should inform a member of staff immediately
- If a student is a victim of abuse of any kind online then they have the option to report this via CEOP as well as to a member of staff. Many websites will have a button for such reporting but students can also copy links and forward them to CEOP directly.
- Do not use the College internet for financial transactions or as a means to run a private business.

General Use

- You must take responsibility for the use of your computer account including your work area. Therefore, you should not disclose the login name or password you have been given to anyone. If you believe your username and password is known by other students then please inform your IT teacher so it can be changed.
- Under no circumstances log in as another user or enter the file areas of other students or staff.
- Your computer storage area (h:\ drive) and College email account is treated as school property. You must understand that your teachers can look through your storage area or email account if required.
- Be polite and appreciate the hard work of the IT technical staff.
- Food or drink is not allowed in the IT rooms for any reason.
- Do not intentionally waste resources by printing unnecessarily.

- As with everywhere in the College the use of strong language, swearing or aggressive behaviour in the IT rooms is not allowed.

- 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.

Breaking any of these rules will result in one or more of the following in accordance with the College disciplinary procedure:

1. Having your network user account disabled either temporarily or, in grave cases, permanently.
2. A letter being sent to your parents/guardians.
3. Appropriate punishments deemed necessary by your Head of House.
4. Suspension and in extreme cases expulsion.

Should you not understand any part of this Acceptable Use Policy, you must seek clarification from one of the IT teachers.

You are strongly encouraged to utilise the College's network resources and if used properly it can be a fun and educationally rewarding experience. These rules are in place for the protection of all the College's users and equipment and are not in place to discourage the use of a great facility.

Student Acceptance of the IT Acceptable Use Policy

I have read and accept the Acceptable Use Policy

Name: .....

Year:

House: ……
Signed: ..... Date: .....

Parent/Guardian Acceptance of the IT Acceptable Use Policy

I have read and understand the IT Acceptable Use Policy.
Child's Name:.....
Year: ……
House: ……
Signed: ..... Date:

Print Name: .....

This form should be completed and returned to the IT Department.