Acceptable Use and E Safety Policy

For the following academies:

St Philip Howard Catholic School

St Mary's Catholic Primary School

Annecy Catholic Primary School

St Joseph's Catholic Primary School

St Paul's Catholic College

This Policy has been approved and adopted by the
Bosco Catholic Education Trust.

Approved:	For review:
October 2020	October 2023

Introduction

The aim for our schools is to create a safe environment where we can both work and learn. This environment should be safe for both young people and adults alike. E-safety is not purely a technological issue. The responsibility for e-safety must not be solely delegated to technical staff, or those with a responsibility for ICT.

We have firmly embedded e-safety within all our safeguarding policies and practices, which are reviewed on a regular basis by those responsible for e-safety, on the school leadership team and the governing body. This then makes that responsibility rest with of all those who work with young people whether in a paid or unpaid capacity.

No one policy or technology can create the safe learning and working environment we need. We work towards this by combining the following:

- Policies and Guidance.
- Technology Based Solutions
- Education in terms of acceptable use and responsibility

Policies

The policies and guidance that help form safe environments for our students to learn and work in include, but are not limited to:

- The school Internet Filtering Policy
- The staff Guidance for the Safer Use of the Internet
- The Behaviour Management Policy
- The Anti Bullying Policy
- The Staff Handbook / Code of Conduct for Staff

Technology

The school provides its own internet filtering solution.

Education

The education of young people is key to them developing an informed confidence and resilience that they need in the digital world.

The National Curriculum programme for ICT at Key Stages 1 to 4 makes it mandatory for children to be taught how to use ICT safely and securely. Together these measures form the basis of a combined learning strategy that can be supported by parents, carers, and the professionals who come into contact with children.

Educating young people in the practice of acceptable use promotes responsible behaviour and builds resilience. Personal, Social and Health Education (PSHE) lessons can also provide an opportunity to explore potential risks, how to minimize these and to consider the impact of our behaviour on others.

We cannot realistically provide solutions to each and every potential issue arising in a rapidly changing world. As a result, young people must be able to transfer established skills and safe working practices to any new "e-activities" they encounter.

We recognise that it is equally important to ensure that the people who care for young people should have the right information to guide and support young people whilst empowering them to keep themselves safe.

The Trust adheres to the e-safety guidance and documentation available on the West Sussex Grid for Learning. The Trust schools complete the '360° safe' - the e-safety self-review tool. This is intended to help schools review their e-safety policies and practice and provides the following:

- Management information that can help the production or review of e-safety policies and develop good practice.
- A process for identifying strengths and weaknesses in your schools' policies and practices.
- Opportunities for commitment and involvement from the whole school.
- A platform for schools to discuss how they might move from a basic level provision for e-safety to practice that is aspirational and innovative.

SHARED ACCESS: ACCEPTABLE USE POLICY

Networked resources, including Internet access and access to the school's Virtual Learning Environment (VLE) are potentially available to students and staff in the school. All users are required to follow the conditions laid down in the policy. Any breach of these conditions may lead to withdrawal of the user's access, monitoring and or retrospective investigation of the users use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

These networked resources are intended for educational purposes and may only be used for legal activities consistent with the rules of the school. Any expression of a personal view about the school or Trust matters in any electronic form of communication must be endorsed to that effect. Any use of the network that would bring the name of the school into disrepute is not allowed.

The school expects that staff will use new technologies as appropriate within the curriculum and that staff will provide guidance and instruction to students in the use of such resources. Independent student use of the Internet or the school's Intranet will only be permitted upon receipt of signed permission and agreement forms as enclosed with this document. All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion.

CONDITIONS OF USE

Personal Responsibility

Access to the networked resources is a privilege, not a right. Users are responsible for their behaviour and communications. Staff and students will be expected to use the resources for the purposes for which they are made available. Users are to take due care with the physical security of hardware they are using. Users will accept personal responsibility for reporting any misuse of the network to the Assistant Headteacher i/c E-safety.

Acceptable Use

Users are expected to utilise the network systems in a responsible manner. It is not possible to set hard and fast rules about what is and what is not acceptable, but the following list provides some guidelines on the matter:

NETWORK ETIQUETTE AND PRIVACY

Users are expected to abide by the rules of network etiquette. These rules include, but are not limited to, the following:

- Be polite – never send or encourage others to send abusive messages.
- Use appropriate language – users should remember that they are representatives of the school on a global public system. Illegal activities of any kind are strictly forbidden.
- Do not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
- Privacy – do not reveal any personal information (e.g. home address, telephone number) about yourself or other users. Do not trespass into other users' files or folders.
- Password – do not reveal your password to anyone. If you think an unauthorised person has learned your password then contact the Assistant Headteacher i/c E-safety.
- Electronic mail – Is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Do not send anonymous messages.
- Disruptions – do not use the network in any way that would disrupt use of the network by others.
- Students will not be allowed access to unsupervised and/or unauthorised chat rooms and should not attempt to gain access to them.
- Students finding unsuitable websites through the school network should report the web address to the Assistant Headteacher i/c E-safety.
- Do not introduce USB Flash Drives into the network without having them checked for viruses.
- Do not attempt to visit websites that might be considered inappropriate. (Such sites would include those relating to illegal activity). All sites visited leave evidence in the county network if not on the computer. Downloading some material is illegal and the police or other authorities may be called to investigate such use.

- Unapproved system utilities and executable files will not be allowed in students' work areas or attached to e-mail.
- Files held on the school's network and internet use will be regularly monitored by ICT technical staff.
- It is the responsibility of the user to take all reasonable steps to ensure compliance with the conditions set out in this Policy document, and to ensure that unacceptable use of the Internet/Intranet does not occur.

UNACCEPTABLE USE

Examples of unacceptable use include but are not limited to the following:

- Sharing user names and ID.
- Using machines logged on under other users' username, students should log off the machine whether they intend to use it or not.
- Accessing or creating, transmitting, displaying or publishing any material (e.g. images, sounds or data) that is likely to cause offence, inconvenience or needless anxiety. (Filters are in place to block e-mails containing language that is or may be deemed to be offensive.)
- Accessing or creating, transmitting or publishing any defamatory material.
- Receiving, sending or publishing material that violates copyright law. This includes through Video Conferencing and Web Broadcasting.
- Receiving, sending or publishing material that violates Data Protection Act or breaching the security this act requires for personal data.
- Transmitting unsolicited material to other users (including those on other networks).
- Unauthorised access to data and resources on the school network system or other systems.
- User action that would cause corruption or destruction of other users' data, or violate the privacy of other users, or intentionally waste time or resources on the network or elsewhere.

Additional guidelines

- Users must comply with the acceptable use policy of any other networks that they access.
- Users must not download software without approval from the Assistant Headteacher i/c IT.

CONSEQUENCES OF UNACCEPTABLE USE

Unacceptable use by students may result in the loss of all computer access for a period of time, as well as possible detentions. An extreme case may result in more severe sanctions including the possibility of exclusion from school. Contact with home will always be made, with the length of sanctions dependent on the specific offence.

SERVICES

There will be no warranties of any kind, whether expressed or implied, for the network service offered by the school. The school will not be responsible for any damages suffered while on the system. These damages include loss of data as a result of delays, non-deliveries, or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the network is at your own risk.

NETWORK SECURITY

Users are expected to inform the Assistant Headteacher i/c E-safety or the Assistant Head i/c IT immediately if a security problem is identified. Do not demonstrate this problem to other users. Users must login with their own user ID and password, where applicable, and must not share this information with other users. Users identified as a security risk will be denied access to the network.

PHYSICAL SECURITY

Portable ICT equipment such as laptops, digital still and video cameras are brought into school at the owner's risk.

WILFUL DAMAGE

Any malicious attempt to harm or destroy any equipment or data of another user or network connected to the school system will result in loss of access, disciplinary action and, if appropriate, legal referral. This includes the creation or uploading of computer viruses. The use of software from unauthorised sources is prohibited.

MEDIA PUBLICATIONS

Written permission from parents or carers will be obtained before photographs of students are published. Named images of students will only be published with the separate written consent of their parents or carers.

Publishing includes, but is not limited to:

- the school website / VLE
- the Local Authority website,
- web broadcasting,
- TV presentations,
- Newspapers – National & Local Students' work will only be published (e.g. photographs, videos, TV presentations, web pages etc.) if parental consent has been given.