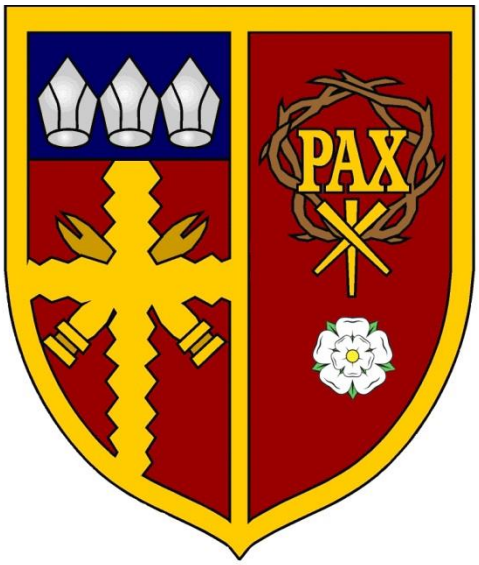
# St. Benedict's Catholic High School




## E-Safety Policy

| Adoption / Review | Committee | Lead Personnel | Review Date |
|---|---|---|---|
| | | | |
| Autumn 2015 | H+S | HT | Autumn 2016 |
| | | | |
| | | | |

# E-SAFETY POLICY

## AIMS

- To ensure that students and staff are able to use the internet and related communication technologies appropriately and safely.
- To build students' and staff resilience to risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.
- To provide the necessary safeguards to manage and reduce risks.
- Help students and staff to be responsible users and stay safe using the internet and other communication technologies for educational, personal and recreational use.
- To safeguard students and staff.

## SCOPE OF THE POLICY

This policy applies to all members of the school community who have access to and are users of school ICT systems – staff, students, volunteers, parents, visitors.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students / 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 / academy, but is linked to membership of the school / academy. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see Behaviour Policy).

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

## CONTEXT

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. They help teachers and students to learn from each other. Young people should have an entitlement to safe internet access at all times. Though the use of these innovative technologies can help to raise educational standards, nevertheless they can also put young people at risk. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images
- Unauthorised access to, loss of, sharing of personal information
- The risk of being groomed by those with whom they make contact on the internet
- Sharing or distribution of personal images without an individual's consent or knowledge  In appropriate communication or contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video or internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of students.
- Staff and students are liable for information that they either write or pass on.

It is impossible to eliminate risks completely. It is therefore essential, through good educational provisions to build students' resilience to the risks to which they may be exposed, so that they have the skills and confidence to deal with these risks.

## ROLES AND RESPONSIBILITIES

### Governors

- Governors are responsible for the approval of the e-safety policy and for reviewing the effectiveness of the policy.
- Governors will appoint a Behaviour and Safety Governor . This role involves regular meetings with the e-safety officer and reporting to the full Governing Body on matters pertaining to e-safety.

### Headteacher

- Ensuring the safety of members of the school community, though the day to day responsibility will be delegated to the e-safety officer.
- Ensure the e-safety officer has access to up to date professional development.
- Make sure there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role.
- Receive regular monitoring reports from the e-safety officer.
- Implement the policy in the event of a serious e-safety allegation being made against a member of staff.

### E-Safety Co-ordinator

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies.
- Liaises with school ICT technical staff.
- Ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety event taking place.
- Ensures that staff are trained and advised on e-safety issues.
- Maintains a log of incidents.
- Meets regularly with the e-safety governor.
- Reports to the Headteacher on e-safety issues.

### Network Manager

- Make sure the ICT infrastructure is secure and not open to misuse or malicious attack.
- Make sure users can only access the school's networks through a properly enforced password protection system.
- Keeps up to date with e-safety technical information.
- Regularly monitors the network in order that any misuse or attempted misuse is reported to Mr Gibson (Acting Headteacher), Mr Smallman (Head of Sixth Form) or nominated E-Safety Governor.

### Teaching and Support Staff

- Have up to date awareness of e-safety matters and read and understood the e-safety policy.
- Have read and understood the Staff Acceptable Use Agreement.
- Report any suspected misuse of problem to the e-safety officer or Head Master.
- Digital communication with students should always be on a professional level and only carried out using school systems.
- Ensure students understand and follow the school e-safety and acceptable use policy.
- Ensure students understand research skills and the need to avoid plagiarism and uphold copyright regulations.
- Monitor ICT activity in lessons
- Be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices.

- In lessons, guide students to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- All new staff should receive e-safety training as part of their induction programme, ensuring they understand the school e-safety policy and Acceptable Use Agreement.
- All staff will have the opportunity to identify e-safety as a training need within the performance management process.
- The e-safety co-ordinator will receive regular updates through attendance at external training sessions and by reviewing guidance documents issued by the DfE and other organisations.

**Designated Senior Lead Person for Child Protection**

Be aware of the potential for serious child protection issues to arise from:

- Sharing personal data
- Access to illegal/inappropriate materials
- Inappropriate on-line contact with adults/strangers
- Potential or actual incidents of grooming
- Cyber-bullying

**Parents/Carers**

- Parents play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way.
- The school will help parents to understand e-safety issues through newsletters, the school website and involvement in local e-safety campaigns.
- Parents should be aware of the school policy on e-safety and the school Acceptable Use agreements.
- The school seeks to provide information and awareness to parents and carers through evening workshops, letters, newsletters and via the school website.

**Students**

- Are responsible for using the school ICT systems in accordance with the Student Acceptable Use Agreement.
- Have a good understanding of personal research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should know and understand school policies on the taking and use of images and on cyber-bullying.
- A planned e-safety programme will be provided as part of the ICT programme
- Assemblies will re-visit the issue of e-safety
- Students, where appropriate, should be taught to be critically aware of the materials they access and be guided to validate the accuracy of information
- Students should be encouraged to adopt safe and responsible use of ICT and to respect copyright when using materials accessed on the internet

**Technical infrastructure**

- The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.
- There will be regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights. Details of the access rights will be recorded by the Network Manager.

- All users will be issued with a username and password by the Network Manager. Users are responsible for the security of their username and password.
- The school maintains and supports a managed filtering service
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems.
- Appropriate security measures are in place to protect servers, firewalls, routers, wireless systems, work stations and hand held devices from accidental or malicious attempts which might threaten the security of the school systems and data.
- Temporary access for guests is available. This has very limited access.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
- The school uses a filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming and chat rooms.

**Use of digital and video images**

- Staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet.
- The school will inform and educate students and staff about the risks associated with the taking, use, sharing, publication and distribution of digital images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- The personal equipment of staff should not be used for taking digital images.
- Care should be taken whilst taking digital/video images that students are appropriately dressed.
- Students and staff must not take, use, share, publish or distribute images of others without their permission, or in the case of student without parental permission.
- Students' full names will not be used anywhere on the website, particularly in association with photographs without first having the permission of parents and the Headteacher.
- Written permission from parents will be obtained before photographs of students are published on the school website.
- The school blocks access to social networking sites in years 7-11.

**E-mail**

- The school email service is regarded as safe and secure and is monitored.
- Users must immediately report to their teacher, E-Safety Officer or the Designated Senior Person for Child Protection the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to such material.
- Any digital communication between staff and students, pupils or parents, must be professional in tone and content.
- Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.
- Email must not be used by staff to transfer information to a third party about students - unless it is within an encrypted, secured email system.

**Protecting Personal Data**

Personal Data will be recorded, processed, transferred and made available according to the Data Protection Act, 1998.

**Responding to incidents of misuse**

- In most cases, the E-safety Officer should be the first point of contact for any complaint.
- Any complaint about staff should be reported to the Headteacher.
- Complaints about cyber-bullying are dealt with in accordance with the school Anti-Bullying Policy.
- Complaints related to Child Protection are dealt with in accordance with the school Child Protection Policy.
- Incidents of mobile phone misuse will be dealt with in accordance with the school Mobile Phone, MP3 & Other Electronic Devices Policy.

**Monitoring and review process**

- The E-safety policy will be reviewed annually.
- The E-safety Officer will monitor the implementation of the policy.
- The Head Master will report to governors about e-safety incidents and any significant new developments in his report to the full Governing Body.

**Linked policies**

Anti-bullying
Behaviour for Learning
Safeguarding
Child Protection

**Policy approved:**

**Policy review date:**

**APPENDIX 1**

## STUDENT ACCEPTABLE USE AGREEMENT

The school has installed computers and internet access to help you with your learning. By signing this agreement you will agree to abide by the rules designed to keep everyone safe. If there is anything that you do not understand, please ask.

- I will not share my password with anyone, or use anyone else's password. If I become aware of another individual's password, I will inform the person and a member of staff.
- I will use a 'strong' password – one that contains letters (upper and lower case), numbers and possibly symbols which I will change on a regular basis.
- I will use school equipment properly and not interfere with the work or data of another student.
- I understand that the school may check my computer files and will monitor the internet sites I visit.
- Before I use or connect my own equipment I will check with a member of staff to see if it is allowed.
- I will use storage devices appropriately.
- I am responsible for all email, chat, sms, blogs, posts, entries on social media etc. that I post or send and will use language appropriate to the audience who may read them. I will be respectful in how I talk to and work with others online and never write or participate in online bullying. I will report any unpleasant material or messages sent to me. I understand my report will be confidential and may help protect other students and myself.
- I know that posting anonymous messages and forwarding chain letters is forbidden.
- Any files attached to an email will be appropriate to the body of the email and not include any inappropriate materials or anything that threatens the integrity of the school ICT system.
- I will not download or bring into school unauthorised programs, including games and music and run them on school computers.
- I will not access inappropriate materials such as pornographic, racist or offensive material or use the school system for personal financial gain, gambling, political purposes or advertising.
- When using the internet or chat room facilities I know that I must not give my home address, mobile phone/telephone number, or arrange to meet someone, unless my parent or carer has given their permission.
- I will always use the terms and conditions when using a site. I know that content on the web is someone's property and I will ask a responsible adult if I want to use information, pictures, video or music or sound to ensure I so not break copyright law.
- I will think carefully about what I read on the internet to question if it is from a reliable source before I use the information.
- I will always credit sources so that I avoid plagiarism.
- I will not make audio, picture or video recordings of another student or teacher without his/her permission.
- I will not attempt to communicate with staff on social media or make any comments which may impact detrimentally upon the school.

**Acceptance of the above agreement**

I have read and understand these rules and agree to them:

Full name of Student Form

Signed by Student Date

**APPENDIX 2**

## STAFF (AND VOLUNTEER) ACCEPTABLE USE AGREEMENT

In order to safeguard students and colleagues it is important that all staff take all possible measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All colleagues have a responsibility to use the school's computer system in a professional, lawful and ethical manner.

- School owned information systems must be used appropriately. I understand that the Computer Misuse Act, 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
- I understand that any hardware and software provided by the school for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
- I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (including letters and numbers).
- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.
- I will ensure that any personal data of students, staff or parents is kept in accordance with the Data Protection Act, 1988.
- I will not keep professional documents which contain school related sensitive or personal information (including images, files or videos) on any personal devices unless they are secured and encrypted.
- I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.
- I will respect copyright and intellectual property rights.
- I have read and understood the school e-safety policy.
- I will report all incidents of concern to the DSL and/or a member of SMT.
- I will not attempt to bypass any filtering and/or security systems put in place by the school. I will report all suspected computer system damage, of virus or other malware to the ICT Network Manager.
- My electronic communications with students, parents and other professionals will only take place via work approved communication channels. Any pre-existing relationships which may compromise this will be discussed with the Head Master.
- I will promote e-safety with students and help them to develop a responsible attitude to safety online, system use and to the content they access or create.
- I understand that my use of the school information systems, internet and email may be monitored.

**I have read and understood, and agree to comply with the staff ICT Acceptable Use Agreement.**

**SIGNED** **PRINT NAME** **DATE**

**APPENDIX 3**

## THE E-SAFETY CURRICULUM Introduction

Teachers have a wider duty of care to raise awareness of e-safety issues within the school. E-Safety is taught at years 6, 7, 8 and 9 and is embedded into the ICT curriculum. Aspects are also covered in other areas of the school, such as in tutor time, assemblies, drop down days, where cyber-bullying is discussed. The school has extensive monitoring of the internet in place, with filtering and blocking of unsuitable websites, chat-rooms and content. Student storage areas and emails are also monitored for unsuitable content, including use of third-party software and games, etc. The overall aim is to make students much more aware of the risks with using the internet, including but not limited to: apps, social networking sites, using email and chatrooms, 'grooming', purchasing online (e-commerce), viruses and spyware, blogging, phishing and premium rate services, cyber-bullying, plagiarism and computing legislation.

### Teaching Overview

| Year | Unit | Topic | Evidence |
|---|---|---|---|
| 6 | ICT Taster Lesson | Safe Use of ICT at school, Game making in Scratch | |
| 7 | Using computers, safely, effectively and responsibly & Understanding computers – Term 1.1 | Logging on, file management, e-safety, email, hardware and software, CPY, binary | Student posters and leaflets on e-Safety. Stay-safe presentations, videos. Student passwords, user area and email organised. |
| 7 | Spreadsheet modelling – Term 1.2 | Creating a financial model, using what if, conditional formatting, creating charts | Worksheets, completed spreadsheet, with formula, functions used appropriately. |
| 7 | Control systems with Flowol- Term 2.1 | Flowcharts, sequencing, sensors, subroutines, actuators, variables | Flowchart for zebra crossing, home automation, pelican crossing, car park. |
| 7 | Introduction to coding through Python- Term 2.2 | Introducing python numbers and arithmetic, selection, writing algorithms, while loops, searching | Development of programs in Python- calculator, ghost game, time tables. |
| 7 | Web Design- Term 3.1 | What makes a good website- audience and purpose, web structure and design, template and page creation, navigation bars and hyperlinks, testing | Research for website, design and development of website. |
| 7 | Graphics- Term 3.2 | Reliability of information on internet- manipulated graphics, introduction to vector graphics, effects and enhancement, adding text | Images before and after, research on images that have been manipulated. |

| Year | Unit | Topic | Evidence |
|---|---|---|---|
| 8 | Using computers, safely, effectively and responsibly & Understanding computers and Networks – Term 1.1 | E-safety, elements of a computer system, binary, the internet, connectivity, types of networks, encryption | Student posters and leaflets on e-Safety. Stay-safe presentations, videos. |
| 8 | Games programming in Scratch – Term 1.2 | Plan, design and develop game in Scratch | Game design, development and evaluation. |
| 8 | Database development – Term 2.1 | Creating tables, queries, form, reports- audience and purpose | Development of table, forms, reports and print screens of queries. |
| 8 | HTML and website development- Term 2.2 | HTML, CSS, design, development, creating a web form | Website research, plan and final website created. |
| 8 | Programming in Python- Term 3.1 | Revise variables, selection (IF), while loops | Development of programs in Python- quiz. |
| 8 | Creating a video & sound manipulation in Audacity- Term 3.2 | Planning, shooting scenes, editing a movie, recording and manipulating sound files, revisit e-safety | Storyboard, finished video with audio. |
| 9 | Computer Crime and cyber security & Understanding computers and networks – Term 1.1 | Legislation: Computer Misuse Act, Copyright and Piracy, Health and Safety at Work, e-safety | Worksheets on various aspects of legislation concerning ICT use, stay safe presentations and videos. |
| 9 | Scratch project- Term 1.2 | Plan, design and develop game in Scratch | Game design, development and evaluation. |
| 9 | Handling data- Term 2.1 | Flat file and relational databases, setting up relationships, macros, picture fields, SQL | Print screen of relationships, macros, SQL, printed table with picture fields. |
| 9 | App development in app shed- Term 2.2 | App vs website, app design and creation, testing | Storyboard, development of app. |
| 9 | Animation in Flash – Term 3.1 | Drawing, buttons, tweening, animation, e-safety recap | Design and development of animation. |
| 9 | Python: Next steps- Term 3.2 | Arrays, procedures, functions | Development of programs in Python |

**APPENDIX 4**

## SAFEGUARDING OF SCHOOL STAFF

## ELECTRONIC COMMUNICATIONS WITH STUDENTS INCLUDING THE USE OF EMAIL AND SOCIAL NETWORKING SITES

All adults employed in the school should:

- Ensure that personal social networking sites are set as private and students should never be listed as approved contacts.

- Never use or access the social networking site of any student unless for investigative purposes (only Heads of Year, Safeguarding Officer or SMT).

- Personal contact details should not be given to students, including mobile telephone numbers. However details could be given to responsible senior students in appropriate circumstances, e.g. in relation to school business or extra-curricular activities.

- Only make contact with students for school-related business, e.g. extra-curricular activities.

- Recognise that text messaging is rarely an appropriate response to a child in a crisis situation or at risk of harm. It should only be used as a last resort when other forms of communication are not possible.

- Not use the internet to send personal messages to a student.

**APPENDIX 5**

## USEFUL WEBSITES

**National Action for Children (NCH)**

| | |
|---|---|
| Parents Guide on Internet usage: | www.nchafc.org.uk/itok/itokhome.html |
| Current activities to promote safe use: | www.nchafc.org.uk/internet |

**Internet Watch Foundation**

| | |
|---|---|
| Report inappropriate websites: | www.iwf.org.uk |
| Safe surfing guide for parents and carers: | www.iwf.org.uk/safe |

**Parents Information Network (PIN):** www.pin.org.uk/learning/safeindex.htm

**Recreational Software Advisory Council (RSACI)**

www.rsac.org