ST BERNARD'S PREPARATORY SCHOOL

ICT: E-SAFETY POLICY

ADVENT 2018

Last review: Advent 2018 Review date: Advent 2019

St. Bernard's Preparatory School

E-Safety Policy

Mission Statement

With God as our shelter and Christ as our guide, the mission of St Bernard's Preparatory School is to educate towards love and service to God, each other and the wider community. Through our broad balanced curriculum we will develop an understanding of each faith and the values we share. We will treat each person with respect, knowing we are special and unique.

The Bernardine Cistercians, believing that Christ is the answer to all human needs and the foundation of all truth, cooperate in the apostolic mission of the Church by their whole monastic life, with its educational work. Their schools endeavour to proclaim Christ through monastic values of prayer, work, community living and unselfish service.

INTRODUCTION

St. Bernard's Preparatory School recognises that ICT and the Internet are excellent tools for learning and communication and can be used in school to enhance the curriculum, challenge students, and support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone in the school community, but it is important that their use is seen as a responsibility and that students, staff and parents use it appropriately and practice good e-safety. It is important that all members of the school community are aware of the dangers of using the Internet and how they should conduct themselves online.

E-safety encompasses internet technologies and electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate children about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

E-safety depends on effective practice at a number of levels:

- Responsible ICT use by the whole school community, encouraged by education and made explicit through this policy
- Sound implementation of e-safety policy in both administration and curriculum, including a secure school network design and use
- Safe and secure broadband including the effective management of filtering.

Writing and reviewing the E-Safety Policy

The E-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT and for child protection. All staff are responsible for e-safety. Our e-Safety Policy has been written by the school. It has been agreed by the staff and Governors. The E-Safety Policy will be reviewed on an annual cycle.

TEACHING AND LEARNING

Why Internet use is important

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience. Internet use is a part of the National Curriculum and a necessary tool for staff and children.

Internet use will enhance learning

The school internet access is designed expressly for pupil use includes filtering appropriate to the age of children. Children will be taught what internet use is acceptable and what is not and given clear objectives for Internet use. Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of children. Staff will guide children in on-line activities that will support the learning outcomes planned for the children's age and maturity.

Children will be taught how to evaluate Internet content

If staff or children discover unsuitable sites, the URL (address), time, date and content must be reported to SLT and the Headteacher. See Appendix 1 for the E-Safety Incident Log.

Staff should ensure that the use of internet derived materials by themselves and by their children complies with copyright law.

Information system security

The security of the school information systems will be reviewed regularly by our Technical Support.

Virus protection is installed and updated regularly. The school currently uses the Sonic Wall TZ500 firewall and filters and Sophos application to control content filtering. Each PC has Webroot anti-virus software installed as a final line of defence.

Technical Support (IForge) is responsible for ensuring:

- That the schools technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required online safety technical requirements and any relevant body online safety policy / guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection.
- Filtering is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- That the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / online safety coordinator for investigation / action / sanction
- That monitoring software / systems are implemented and updated as agreed in school policies
- The security of the school information system is reviewed regularly.

Published content and the school web site

Contact details are on our school website: school address, e-mail and telephone number. Staff or children's personal information will not be published. The Headteacher, who is also the Designated Child Protection Officer will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing children's images and work

Photographs that include children will be selected carefully. Photographs must only be taken on a camera provided by the school. Children's full names will not be used anywhere on the website, particularly in association with photographs. Written permission is sought from parents with regards to photographs of their child being published on the school website.

Social networking and personal publishing

Children are advised about the use of social networking sites out of school and never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc. Children and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged children.

Cyber-bullying

Cyber-bullying by children will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures which are outlined in our Anti-Bullying Policy Information about specific strategies or programmes in place to prevent and tackle bullying is set out in the Behaviour Policy**.** The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to members of the school community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action. If an allegation of bullying does come up, the school will:

- Take it seriously
- Act as quickly as possible to establish the facts. It may be necessary to examine school systems and logs or contact the service provider in order to identify the bully
- Record and report the incident
- Provide support and reassurance to the victim
- Make it clear to the 'bully' that this behaviour will not be tolerated. If there is a group of people involved, they will be spoken to individually and as a whole group. It is important that children who have harmed another, either physically or emotionally, redress their actions and the school will make sure that they understand what they have done and the impact of their actions.

If a sanction is used, it will correlate to the seriousness of the incident and the 'bully' will be told why it is being used. They will be asked to remove any harmful or inappropriate content that has been published and the service provide may be contacted to do this if they refuse or are unable to remove it. They may have their Internet access suspended in school.
Repeated bullying may result in fixed-term exclusion.

.**Managing emerging technologies**

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Children are not permitted to have mobile phones in school.
Staff adhere to our Mobile Phone and Camera Policy.

POLICY DECISIONS

Authorising Internet access

All staff must read and sign the Acceptable ICT use Statement. At Key Stage 1 and Early Years, access to the internet will be by adult demonstration or directly supervised access to specific, approved on-line materials.

Assessing risks

In common with other media such as magazines, books and video, some material available via the

Internet is unsuitable for children. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school can accept liability for the material accessed, or any consequences of Internet access.

Handling e-safety complaints

Complaints of Internet misuse will be dealt with by a member of the SLT.

Any complaint about staff misuse must be referred to the head teacher.

Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

All e-safety incidents will be recorded in the E-Safety Incident Log by a member of SLT (see Appendix 1).

Communicating School Policy

Introducing the e-safety policy to children

Rules for internet access are posted in the Amrit Mann Room. Children will be informed that Internet use will be monitored. Advice on e-Safety is introduced at an age-appropriate level to raise the awareness and importance of safe and responsible internet use and taught as an ongoing area of the ICT Curriculum.

Staff and the E-Safety policy

All staff are given our E-Safety Policy and its importance explained. Staff are aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential at all times.

Enlisting parents' / carers' support

Our E-Safety Policy will be published on the school website

Protecting Personal Data

St Bernard's Preparatory School believes that protecting the privacy of our staff and children and regulating their safety through data management, control and evaluation is vital to whole-school and individual progress. The school collects personal data from children, parents, and staff and processes it in order to support teaching and learning, monitor and report on children and teacher progress, and strengthen our pastoral provision. In line with the Data Protection Act 1998, and following principles of good practice when processing data, the school will:

- Ensure that data is fairly and lawfully processed
- Process data only for limited purposes
- Ensure that all data processed is adequate, relevant and not excessive
- Ensure that data processed is accurate
- Not keep data longer than is necessary
- Process the data in accordance with the data subject's rights
- Ensure that data is secure
- Ensure that data is not transferred to other countries without adequate protection.

There may be circumstances where the school is required either by law or in the best interests of our children or staff to pass information onto external authorities; for example, our local authority, ISI, DfE or the Department of Health. These authorities are up-to-date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

For more information on the school's safeguards relating to data protection read our Data Protection Policy.

Roles and Responsibilities

Key personnel

The Designated Safeguarding Lead (DSL) for child protection is Mr N Cheesman
Contact details: email: headteacher@stbernardsprep.org tel: 01753 521821

The Deputy Designated Lead is Mrs S Bascombe
Contact details: email: sbascombe@stbernardsprep.org tel: .01753 521821

The nominated child protection governor is Ms A-M McIntosh
Contact details: email: mcintosh@nores.org.uk

The Computing co-ordinator is Mrs A Rafferty
Contact details: email: arafferty@stbernardsprep.org tel: 01753 521821

Applies to:
Whole School including Early Years Foundation Stage (EYFS), all staff, peripatetics, clubs and extra-curricular activity providers, volunteers, Trustees, Governors.

Availability:
This policy is made available to parents on the website www.st-bernardsprep.org or a copy may be requested from the school office.

Related policies:
Safeguarding Portfolio, Behaviour Policy, Curriculum Policy, Health and Safety Policy, Premises Management Documents, Data Protection Policy, Staff Induction, Staff Handbook, Website Terms and Conditions, Mobile Phone and Camera

Monitoring and Review
This policy will be subject to continuous monitoring, refinement and audit by the Headmaster.
The Trustees will undertake a formal annual review of this policy for the purpose of monitoring and of the efficiency with which the related duties have been discharged or earlier if significant changes to the systems and arrangements take place, or if legislation, regulatory requirements or best practice guidelines so require.

Signed by _____

Headmaster_____ Date_____

Chair of Governors_____ Date_____

Last review: Advent 2016 Review date: Advent 2018

Appendix 1: E-Safety Incident Log

Details of all e-safety incidents must be recorded by a member of SLT. This log will be monitored by the Headteacher and Chair of Governors.

DATE & TIME	NAME OF PUPIL OR STAFF	MALE OR FEMALE	ROOM & COMPUTER/DEVICE NUMBER	DETAILS OF INCIDENT (INCLUDE EVIDENCE)	ACTIONS & REASONS9

Appendix 2: Acceptable Internet Use Policy and Statement Lent 2017

The computer system is owned by St Bernard's Preparatory School and is made available to staff to enhance staff's professional activities including teaching, research, administration and management. The schools Acceptable Internet Use Policy has been drawn up to protect all parties – the staff, students, governors, visitors and the school.

The school reserves the right to examine or delete any files that may be held on its computer system and to monitor any Internet sites visited. Activity that threatens the integrity of the school ICT systems, or that attacks or corrupts other systems, is forbidden. Sites and materials accessed must be appropriate to work in school. Users will recognise materials that are inappropriate and should expect to have their access removed. The same professional levels of language and content should be applied as for letters or other media, particularly as e-mail is often forwarded.

This policy outlines what are acceptable and unacceptable uses of ICT facilities within St. Bernard's Preparatory School. Whilst we aim to support the full use of the vast educational potential of new technologies, we also have a responsibility to provide safeguards against risk, unacceptable material and activities. These guidelines are designed to protect children, staff and visitors from e-safety incidents and promote a safe e-learning environment for children.

At St. Bernard's Preparatory School we believe that children should be trusted to use digital technologies in a principled and productive way. The general spirit of this policy is about giving everyone the opportunity to make productive decisions in the ways they decide to use digital technologies; we should all be fully engaged in the on-going debate about what responsible digital citizenship means and how we can nurture it within our school.

Examples of acceptable use are:

- Using web browsers to obtain information from the Internet.
- Accessing databases for information as needed.
- Using e-mail for contacts.
- Using the school's network to promote the exchange of information to further education and research and is consistent with the mission of the school.
- Using the school's network to access outside resources that conform to this "Acceptable Use Policy".
- Using the network and Internet in a manner, which respects the rights and property of others.
- Keeping all accounts and passwords confidential and inaccessible to others.
- Showing responsibility by making backup copies of material critical to you.
- Showing responsibility by taking precautions to prevent viruses on the school's equipment.
- Upon receipt of an attachment checking to making sure it is from a known source.
- Backing out of an accidentally encountered site that contains materials that violate the rules of acceptable use, and notifying a teacher or supervising adult of the occurrence immediately.
- Logging out or locking computers when they are left unattended
- Recognise that electronic communications sent through or stored on the school's network will be treated as school related and may be monitored or examined by the Headteacher or her/his authorised delegates for operational, maintenance, compliance, auditing, security and/or investigative purposes
- Reporting any damage to or loss of computer hardware immediately
- Saving documents onto appropriate storage areas of the school network or other appropriate storage systems

- Reporting any inappropriate behaviour and online bullying to a member of staff and the ICT Coordinator
- Take reasonable care that there is no damage or loss of any equipment on loan from school

Examples of unacceptable use are:

- Use of the Internet for purposes that are illegal, unethical, harmful to the school, or non-productive.
- Sending or forwarding chain e-mail, i.e., messages containing instructions to forward the message to others.
- Recording, filming or taking photographs on school premises without permission and without the consent of parents or carers.
- Broadcasting e-mail, i.e., sending the same message to more than 10 recipients or more than one distribution list.
- Relocating school information and communication equipment without prior permission
- Conducting a personal business using school resources.
- Transmitting any content that is offensive, harassing, or fraudulent.
- Using inappropriate language: do not swear, use vulgarities or sexual innuendos.
- The sending of material likely to be offensive or objectionable to recipients.
- Using programs that harass school users or infiltrate a computing system and/or damage the software components is prohibited.
- Changing original software setting/configuration of school owned computers
- Doing harm to other people or their work.
- Installing software on school computers unless authorised by the ICT Team.
- Doing damage to the computer or the network in any way.
- Interfering with the operation of the network by installing illegal software, shareware, or freeware.
- Plagiarisation and violation of copyright laws.
- Conversation in email using all upper case letters. This is considered shouting.
- Sharing your passwords with another person. Doing so could compromise the security of your files.
- Wasting limited resources such as disk space or printing capacity.
- Trespassing in another's folders, work, or files.
- Removing software CDs from their rightful location
- Giving out personal information such as your home address or telephone number. Use the school's address instead, but not the school's phone number.
- Downloading material from the Internet without specific authorisation from a teacher or assistant.
- Viewing, sending, or displaying offensive messages or pictures.
- Accessing sites that contain pornography; that spread hatred; that promote discrimination; that give instruction for acts of terrorism, harassment, murder, suicide, or other illegal activity.
- Use for personal financial gain, gambling, political purposes, advertising or social media for such purposes is forbidden.

All staff should sign a copy of this **Acceptable Internet Use Policy and Statement** and return it to the ICT Coordinator.

I understand the guidelines and agree to follow them.
Name:_____Signed:_____

Date: _____