Classification:

Public

E-Safety and Acceptable Use

Bishop Perowne
Church of England College
Endeavour Forever

Title: E-Safety and Acceptable Use

Document Type: Policy and Procedure

Document Reference: SWC-02

Version: 1.0

Status: Approved

Bishop Perowne Church of England College, Merriman's Hill Road, Worcester, Worcestershire, WR8 9LE | www.bishopperowne.co.uk
T: 01905 746800 | F: 01905 746846 | E: info@bishopperowne.co.uk

Table of contents

1 OVERVIEW

1.1 Purpose

Refer to Section 3 Policies and Procedures

1.2 Scope

Refer to Section 3 Policies and Procedures

1.3 Related documents

- Safeguarding and Child Protection
- Student Behaviour Discipline and Rewards

1.4 Reviews

Refer to Section 3 Policies and Procedures

1.5 Equality Impact Assessment

Under the Equality Act 2010 the College is obliged not to discriminate against people on the basis of age, disability, gender, gender identity, pregnancy or maternity, race, religion or belief and sexual orientation.

This policy has been equality impact assessed and the Governing Board believes that it is in line with the Equality Act 2010 as it is fair, it does not prioritise or disadvantage any student or any other connected party and it helps to promote equality at the College.

2 RESPONSIBILTY FOR THE POLICY AND PROCEDURE

2.1 Role of the Governing Board

The Governing Board has:

- delegated powers and responsibilities to the Head teacher to ensure all college personnel and visitors to the college are aware of this policy;
- responsibility for ensuring this policy and all policies are maintained and updated regularly;
- responsibility for ensuring all policies are made available to parents;
- nominated a link governor to visit the college regularly, to liaise with the Head teacher and the coordinator and to report back to the Governing Board;
- responsibility for the effective implementation, monitoring and evaluation of this policy

2.2 Role of the head teacher

The Head teacher will:

- ensure all College personnel, students and parents are aware of this policy;
- work closely with the link governor and coordinator;
- provide guidance, support and training to all staff;
- monitor the effectiveness of this policy;

3 POLICY AND PROCEDURES

The school's e-safety policy operates in conjunction with other policies including those for behaviour and safeguarding.

3.1 Aim

We recognise the value of modern technology systems and welcome their development. We continually strive to enhance their appropriate use (both within school and outside) in order to promote the educational attainment of our students. This policy is of paramount importance as our students' access to technology is currently becoming universal and increasingly more mobile.

The technologies encompassed by this policy include all computer and Internet technologies and electronic communication devices such as mobile phones and tablets.

Any cases of a breach of the policy will be referred to the ELT member responsible for IT systems.

Internet usage: The internet is used within the school to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

We recognise the importance of the internet as an essential element in 21st century life for education, business and social interaction. Access to the internet is therefore an entitlement for students who show a responsible and mature approach to its use.

Students will use the internet outside of school and part of our responsibility is to educate them in safe use of the technology.

The breadth of issues classified within e-safety is considerable, but the three areas of risk we prioritise when talking to students are as follows:

Content (being exposed to illegal, inappropriate or harmful material, extremist propaganda or any site promoting radicalisation).

Common risks we address with students within content focus on exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist

language) and substance abuse. We also focus on lifestyle websites, for example pro-anorexia/ selfharm/ suicide sites, and so-called "hate sites". Equally, we believe that it is important that students are taught to check the authenticity and accuracy of any online content they look at.

Contact (being subjected to harmful online interaction with other users).
Dangers we address with students here include grooming, all forms of cyber-bullying, as well as identity theft (including so-called "frape", the hacking of Facebook profiles) and password security.

Conduct (personal online behaviour that increases the likelihood of, or causes harm).

Within this area, students are taught about privacy issues, including disclosure of personal information, as well as digital footprint and online reputation. They are also taught about the need to consider health and well-being, where necessary limiting the amount of time spent online (internet or gaming). Equally, we believe it is important that students are educated about the dangers of sending or receiving personally intimate images, and of infringing music and film copyright laws.

3.2 Use of internet within the School

Amongst the uses of the internet within school are the following:

- Access to learning wherever and whenever convenient. Access to world-wide education resources including museums and art galleries.
- Educational and cultural exchanges between students world-wide.
- Access to experts in many fields for students and staff.
- Professional development for staff through access to national developments, educational materials and effective curriculum practice. Collaborations across support services and professional associations.
- Improved access to technical support including remote management of networks and automatic system updates.
- Exchange of curriculum and administration data with the Local Authority and DFE.

3.3 Student safety on the school internet system

- The school Internet facility has been designed expressly for student use and includes filtering (Sonicwall) appropriate to the age of students.
- Impero monitoring software is employed in all IT rooms
- Impero keyword logging is deployed throughout the school

- Students are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access is planned to enrich and extend learning activities.
- Staff guide students in on-line activities that will support learning outcomes and plan for the students' age and maturity.
- Students are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

3.4 Gaining access to the school internet

- The school maintain a current record of all system users (including staff and students) who are granted Internet access.
- All staff and governors with access to ICT facilities must read and accept the 'ICT Acceptable Use Policy for Staff' before using any school ICT resource.
- All students must read and accept the 'Student ICT Acceptable use policy' before using any school ICT resource.

3.5 Inappropriate usage of internet and loss of privilege

Any member of staff or student in breach of the agreement for usage of the Internet will have their access curtailed immediately pending investigation. Appropriate sanctions will be taken in accordance to the severity of the breach.

3.6 Social Networking Sites

Access to Social Networking sites (for example Twitter, Bebo, Facebook, Orkut, Friendster, MSN and MySpace) is forbidden on school hardware and all such sites are blocked.

YouTube is accessible and utilised as a teaching tool in various subject areas such as Music.

Students using such sites outside of school have a duty to use them responsibly. Any incident of slander, abuse or defamation perpetrated on a social networking site which impacts upon one of our students, shall be treated as bullying and shall be sanctioned in accordance with the school's behaviour policy.

It is our policy to allow students to have a mobile phone with them in school should they choose to do so under the conditions outlined in mobile phone policy:

3.7 School Website

- The contact details on the website are the school address, e-mail and telephone number. Staff or student personal information is not and shall not be published.
- Currently the headteacher has overall editorial responsibility and ensures that content is accurate and appropriate.

3.8 Curriculum themes and topics

- Photographs that include students will be selected carefully and will be appropriate for the context.
- Students' full names will only be used when featured on news articles sent to press.
- No photographs of students are published on the school website without permission from the parent/carer.
- Student work can only be published with the permission of the student

3.9 Information system security

- School ICT systems' capacity and security are reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with IT technical experts.

3.10 Protecting Personal Data

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

3.11 Assessing risks

The school takes all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school can accept no liability for the material accessed, or any consequences of Internet access.

3.12 Handling of E-safety complaints

- Any complaint about staff misuse must be referred to the ELT member responsible for ICT systems.
- Any complaint about student misuse must be referred to the IT manager in the first instance.

- Complaints of a child protection nature must be dealt with in accordance with the school's safeguarding procedures.

3.13 Communication of Policy

Students

- Rules for Internet access are posted in the ICT rooms and Study Centre.
- Students are informed that Internet use will be monitored.
- Students sign an acceptable use document (See Appendix B)

Staff

- All staff are issued with this policy and its importance is explained. The policy is also available on the school website.
- Staff are made aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff who manage filtering systems or monitor ICT use are supervised by the Leadership Team and have clear procedures for reporting issues.

Parents / Carers

- Parents' attention is drawn to the e-Safety Policy in newsletters and on the school website. • Parents sign an acceptable use document (see Appendix B)

4 DISSEMENATION

4.1 Promoting Awareness

We will raise awareness of this policy via:

- The College website www.bishopperowne.co.uk
- Meetings with College personnel and volunteers
- Reports such as the annual report to parents and Head teacher reports to the Governing Board

4.2 Training

All school personnel:

- Receive training on induction which specifically covers: ○ All aspects of this policy
- Receive periodic training so that they are kept up to date with new information;
- Receive equal opportunities training on induction in order to improve their understanding of the Equality Act 2010 and its implications.

4.3 Monitoring the Effectiveness of the Policy

This policy will be reviewed annually or when the need arises.

5 GLOSSARY

Glossary of terms used within this policy and procedure document. For the full Glossary of terms used at Bishop Perowne CE College, please refer to the document "REF-02 Glossary of Terms".

P	
PE	Physical Education
PSHE	Personal, social, health and economic education

R	
RE	Religious Education

Appendix A: Student ICT acceptable use Information and guidance

We offer all our students a wide variety of ICT resources which are under constant improvement and development. They are offered access to the Bishop Perowne Church Of England College network, internet and electronic mail (email). Keeping our students 'safe' on the internet and supporting them to use the network appropriately is one of our key responsibilities. As a consequence we operate a 'Student ICT Acceptable Use Policy' and hope that parents/carers will support us. The 'Student ICT Acceptable Use Policy' will be explained to all new students during their first 2 weeks in school and then reiterated annually. Access to the Bishop Perowne Church Of England College network, internet and electronic mail (email) will stop once students have left the school.

At the outset we must emphasise that the majority of our students use the network, internet and electronic mail (email) safely and sensibly and this document acts to increase awareness for all. We take any infringement of the 'Student ICT Acceptable Use Policy' very seriously and have installed software to monitor the use of the network, internet and email. Any case reported will be thoroughly investigated and judged on an individual basis. Students should expect serious sanctions to apply.

As part of the school's ICT programme, we offer students supervised access to the internet. Before the school allows students to use the internet, they must obtain permission from their parent/carer. Various projects have proven the educational benefits of internet access, which enables students to explore thousands of libraries, databases, and bulletin boards. They will also be able to exchange messages with other learners throughout the world.

It is the school's policy that every reasonable step should be taken to prevent exposure of students to undesirable materials/contacts on the internet, including extremist propaganda or any site promoting radicalisation of any sort. It is recognised that this can happen not only through deliberate searching for such materials, but also unintentionally when a justifiable internet search yields unexpected results. To reduce such occurrences, the school has adopted filtered access via the Local Authority. This facility stops students accessing sites deemed inappropriate for use at school and also provides a full audit trail. We believe that the benefits to students from access to the internet exceed any disadvantages. However, as with any other area, parents/carers are responsible for setting and conveying the standards that their sons/daughters should follow when using media and information sources. The school therefore supports and respects each family's right to decide whether or not to apply for access. During school, teachers will guide students towards appropriate material. At home, families bear the same responsibility for guidance as they exercise with other information sources such as television, telephones, films and radio.

YouTube, Bebo, Facebook, Twitter, Orkut, Friendster, MSN and MySpace. These are the names of well known and popular websites many people - adults and children - will probably have come across. When used positively they allow people to share music, video, art, opinion, collaborate on work or indeed just have social discussions. Most of the content is harmless; other content can be cruel and cutting. The sites are not rigorously censored in terms of content. For example, on YouTube the BBC is putting video trailers for its forthcoming TV programmes whilst other contributors are posting more inappropriate material. The other sites allow 'members' to write about themselves, and other people of course. Not all of it is appropriate.

Anyone can view the content on YouTube, although for access to some sites users have to register details on the site. MySpace requires the user to sign up immediately and Bebo lets you see some material but expects you to join in order to use more of the functionality.

Access to these sites is very easy. For students, having their own 'social networking' space is a very popular thing to have, but both parents/carers and students aren't always aware of the risks they face when using sites like Facebook, MySpace or Bebo. One of the rules that you may not be aware of is the minimum age for the sites: 13 for signing up to Bebo, 13 for Facebook and 14 for MySpace. Also it is worth remembering that these are public spaces which anyone can view and use the information how they please. Your son/daughter may already be a member of them and a contributor, not just a reader of material. That means they have access to material which you may well consider inappropriate. The users of these sites have the ability to create their own material and post whatever they like on to their site i.e. films, images or text. As it is accessed solely by user identification and a password, it is their choice who views it and whom they choose to pass it to.

Here are the main e-safety issues which should be discussed with your son/daughter:

- **Personal Identity Fraud**: there is a concern if students post personal details or complete online surveys. They should avoid giving out their full name, mailing address, telephone number, the name of their school, or any other information that could help someone determine their actual identity.
- **Public Domain Information:** all images, comments are stored and made available to the public. There are privacy settings and they should be used.
- **Online Bullying:** this can be in the form of comments, blog entries and chat rooms.
- **Exploitation/ Misrepresentation:** clearly people may try to make contact with students and they may not be who they say they are. Students should never meet anyone they have met online.

You know your son/daughter best. Visit the sites and see for yourself what's being said and the potential of what could be said or shown. Ask your son/daughter if they use the sites at all. If so you might engage in a discussion with them about the issues we have highlighted above. The websites can be useful and are a part of life nowadays. However educating our children on the issues will mean they can use them safely.

Electronic mail (email) provides a quick and effective means of communication. Students must be made aware that they will be held responsible for the content of any email message they transmit and that they should not contain messages using language or content that is unacceptable. It is also recognised that some people may try to use email to identify and contact students for unacceptable reasons.

The following points should be supported at all times:

- Steps should be taken to verify the identity of any school, organisation, adult or child seeking to establish regular email with the school or its students.
- Students should avoid revealing their identification within email messages. Students should only be identified by their network username and the student's own address is never revealed.
- Information should never be given that might reveal a student's identity or their current whereabouts.

We also have a number of leaflets from national bodies that explain issues further and also cover internet use at home. If you would like copies of these, please contact the school. Further information about e-safety can be found at

www.thinkuknow.co.uk General online safety www.chatdanger.com Using chat rooms, mobile phones and email safely www.blogsafety.com Using blogs and social networking

This document aims to outline the key aspects of using the ICT facilities but if you require any further advice please contact the school.

Appendix B: ICT Acceptable Use Policy for Students

Aims

The aims of this Acceptable Use Policy are:

- To ensure that students may benefit from the learning opportunities offered by the school's network and internet resources in a safe and effective manner.
- To protect the school's ICT infrastructure from misuse and attack.

The school undertakes to:

- Prioritise Data Protection and adhere to strict guidelines on the use of personal or sensitive information.
- Provide a safe and productive digital learning environment
- Provide students with training in the area of internet safety
- Supervise students' network and internet access wherever possible
- Monitor students' network and internet activities using software systems
- Provide internet filtering (Sonicwall) in order to minimise the risk to inappropriate material
- Ensure there is a secure and regular backup of student data wherever possible. Nevertheless, students are still primarily responsible for backing up their own data and work.
- Ensure that robust and up to date virus detection and security systems are in place to protect students' data.
- Only publish students' projects, artwork or school work on the School Website/Internet in line with agreed school policy.

Important information for all students:

- Use of ICT Facilities is forbidden unless supervised by a member of staff
- Network and Internet use and access is considered a school resource and a privilege
- If the school AUP is not adhered to, this privilege will be withdrawn and appropriate sanctions will be imposed.
- Designated staff can review student files and communications to ensure that the system is being used responsibly. They also have the right to access computer storage areas, accounts and removable media, including USB Flash Drives and CD-ROMs
- Designated members of staff can remotely view a student's computer screen at any time, without them knowing, in order to ensure compliance and appropriate use of the Bishop Perowne network.
- Students are subject to the provisions of the Copyright, Designs and Patents Act 1988;

- The school will provide information on the following legislation relating to use of the Bishop Perowne network, which teachers, students and parents/carers should familiarise themselves with: The Data Protection Act 1998; Data Protection (Amendment) Act 2003; Video Recordings Act 1989; Copyright, Designs and Patents Act 1988; and Computer Misuse Act 1990.

Students will:

- Ask a teacher before using any personal USB flash drive, CD-ROM or similar device in school.
- Observe good etiquette at all times and behave in a way that reflects well on them and the school.
- Use the Bishop Perowne network for school related matters only, use computers for educational purposes and adhere to the student print policy.
- Make sure they take regular backups of their work.
- Respect other computer users and never harass, harm, cause insult or offence.
- Respect the security protocols in place on the computers and not attempt to bypass or alter security settings put in place on the Bishop Perowne network. Attempting to bypass or breach the school security systems is a serious offence.
- Use approved school email accounts for school use only. Personal email accounts such as hotmail and gmail are prohibited.
- Only use discussion forums or other electronic communications that have been approved by the school.
- Report any damaged ICT equipment (accidentally or otherwise) to the supervising member of staff immediately.
- Read and adhere to school information on e-Safety, cyber-bullying and social networking guidance.

Students will NOT:

- Attempt to upload, download or transfer any software from the internet or portable media.
- Attempt to bypass the school's internet filters (Sonicwall). Violation of this is a serious offence.
- Copy software or multimedia content unless it has been approved by a member of staff.
- Install, attempt to install, or store programs of any type on the Bishop Perowne network.
- Use the internet, computer systems, portable media or other mobile devices for playing non-educational games.
- Store personal photographs, music, games or other prohibited/inappropriate content in their user area (N: Drive) or anywhere on the school network.
- Damage, disable, dismantle or otherwise cause, or attempt to cause harm to the operation of computers, or any other ICT equipment or cables.

- Attempt to connect mobile equipment (e.g. laptops, tablets, PSPs, mobile phones etc.) to the school network.
- Eat or drink in any room where there is ICT equipment.
- Reveal their password to anyone, or use someone else's username or password. Students are responsible for the actions of anyone who is using their username and password, so must immediately tell a member of staff if they suspect that someone else has this information.
- Access or alter other people's folders, work or files without permission.
- Visit Internet sites that contain obscene, illegal, hateful or otherwise objectionable materials, including any website containing any form of extremist propaganda or promotion of radicalisation. Any such sites should be reported to a member of staff immediately.
- Send or receive any material that is illegal, obscene, defamatory or intended to annoy or intimidate another person.
- Use social networking sites, such as Twitter or Facebook while in school, or use such platforms to make public comments about Bishop Perowne Church Of England College, its staff or students, which are defamatory, liable to cause offense or bring the school into disrepute.
- Pass personal information on (like real names or addresses) to anyone on the internet.

Bishop Perowne
Church of England College
Endeavour Forever

Bishop Perowne
Church of England College
Endeavour Forever

Any enquiries regarding this publication should be sent to us at

Bishop Perowne C. of E. College,
Merriman's Hill Road,
Worcester,
Worcestershire,
WR3 8LE

T: 01905 746800
F :01905 746846
E: info@bishopperowne.co.uk

This document is also available from our website at www.bishopperowne.co.uk