ST BRENDAN'S
SIXTH FORM COLLEGE

E - SAFETY POLICY

This policy was adopted by the Governing Body in June 2011.
It was reviewed and updated at the Personnel Committee on 13th June 2013.

Table of Contents Page

1. Introduction 3

2. Creation, Monitoring and Review 3

3. Policy Scope 3

4. Roles and Responsibilities 4

5. Risk Assessment 5

6. Behaviour 5

7. Use of Images and Video 6

8. Communication with Students 6

9. Personal Information 6

10. Education and Training 7

11. Incidents and Response 8

12. Feedback 8

13. Further Information 8

1. Introduction

1.1 St Brendan's Sixth Form College recognises the benefits and opportunities which new technologies offer to teaching and learning. We encourage the use of technology in order to enhance skills and promote achievement. However, the accessible and global nature of the internet, and variety of technologies available, mean that we are also aware of potential risks and challenges associated with such use.

1.2 Our approach is to implement safeguards within the College and to support staff and students to identify and manage risks independently. We believe this can be achieved through a combination of security measures, training and guidance and implementation of our associated policies. In furtherance of our duty to safeguard students, and to advance equality and tackle discrimination, bullying and harassment, we will do all that we can to make our students and staff E-Safe and to satisfy our wider duty of care.

1.3 This E-Safety Policy should be read in conjunction with other relevant College policies e.g. Safeguarding Policy, Preventing Bullying and Harassment Policy, Information, Communication and Data Technology Policy, and, in particular, the ICT Acceptable Use Policies for Staff and Students.

2. Creation, Monitoring and Review

2.1 This policy was originally written by the E-Safety Officer after consultation with members of staff and students. It was approved by the College Management Team and College Governors in June 2011.

2.2 The impact of the policy will be monitored regularly by the Safeguarding Committee, to ensure it captures issues relating to new technologies and trends, and it will also be reconsidered where concerns are raised by the E-Safety Officer or where an E-Safety incident has been recorded. The Policy will be reviewed by the Personnel Committee at least every two years.

3. Policy Scope

3.1 The policy applies to all members of the College community who have access to the College IT systems, both on the premises and remotely. Any user of College ICT systems must adhere to and sign a hard copy of the ICT Acceptable Use Policy for Staff (including the Acceptable Use of Social Media Policy).

3.2 This Policy covers all forms of electronic communication, internet usage etc. on site, and any off site used for College business or that might affect the College's reputation. It applies to the use of all internet and electronic communication devices such as laptops, mobile phones, Blackberries, games consoles and tablets.

4. Roles and Responsibilities

4.1 There are clear lines of responsibility for E-Safety within the College. The Safeguarding Officer is the designated person for all matters relating to E-Safety.

4.2 It is important, however, to note that **all staff are responsible for ensuring the safety of students** and should report any concerns immediately to their line manager. When informed about an E-Safety incident, staff members must take particular care not to guarantee any measure of confidentiality towards either the individual reporting it, or to those involved.

4.3 All students must know what to do if they have E-Safety concerns and who to talk to. In most cases, this will be their Pastoral Support Assistant. Where any report of an E-Safety incident is made, all parties should know what procedure is triggered and how this will be followed up. Where appropriate, the Designated Safeguarding Officer may intervene with appropriate additional support from external agencies.

4.4 E- Safety Officer:

The E-Safety Officer (who is also the Safeguarding Officer and Assistant Principal) is responsible for leading the E-Safety policy and procedures, raising issues with the Safeguarding Committee, delivering staff development and training, recording incidents, reporting to the Senior Leadership Team (SLT) and Governors, and liaising with external agencies to promote E-Safety within the College community. The E-Safety Officer may also organise workshops or communication with students or parents/ carers on E-Safety issues. .

4.5 Students:

Students are responsible for using the College ICT systems and mobile devices in accordance with the College’s ICT Acceptable Use Policy, which they must agree to, and sign at enrolment. They are expected to seek help and follow procedures where they are worried or concerned, or where they believe an E-Safety incident has taken place involving them or another member of the College community. Students must act safely and responsibly at all times when using the internet and/or mobile technologies.

4.6 Staff:

All staff are responsible for using the College ICT systems and mobile devices in accordance with the College Acceptable Use Policy for Staff, which they must sign during their induction, and which they must actively promote through embedded good practice. Staff are responsible for attending staff training on E-Safety and acting as role models to students at all times.

All staff should implement relevant College policies and understand the incident reporting procedures. Any incident of unacceptable practice that is discovered by a staff member must be reported to the E-Safety Officer and/or line manager without delay. If a staff member is a victim of cyber-bullying, this should also be reported to the E-Safety Officer in the first instance.

4.7 Governors

Governors are responsible for reviewing the Policy, and monitoring its implementation through the Safeguarding Annual Report.

4.8 IT Manager

The IT Manager will take the lead in ensuring that the College network is safe and secure. Every effort will be made to keep security software up to date. Appropriate security measures will include the use of enhanced filtering and protection of firewalls, servers, routers, work stations etc. to prevent accidental or malicious access of College systems and information. Digital communications, including email and internet postings, over the College network, will be monitored in line with the ICT and Data Technology Policy.

5. Risk Assessment

Any potential College wide issue arising from E-Safety will be added to the College's Risk Register.

6. Behaviour

6.1 St Brendan's College will ensure that all users of technologies adhere to the standard of behaviour as set out in the E-Safety and ICT Acceptable Use Policy.

6.2 The College will not tolerate any abuse of ICT systems. Whether offline or online, communications by staff and students should be appropriate, courteous and respectful at all times.

6.3 Any reported incident of bullying or harassment (e.g. cyber- bullying) will be dealt with under the Preventing Bullying and Harassment Procedures. If it is deemed that a student is at risk of significant harm, the matter will be passed to the Designated Safeguarding Officer and dealt with under that referral process.

Other unacceptable conduct will be treated seriously and in line with the student and staff disciplinary codes. Where conduct is found to be unacceptable, the College will usually deal with the matter internally. Where conduct is considered illegal, the College will report the matter to the police and/or relevant external agencies.

7. Use of Images and Video

7.1 The use of images, or photographs, video clips, is popular in teaching and learning and should be encouraged where there is no breach of copyright or other rights of another person. This will include images downloaded from the internet and images belonging to staff or students.

7.2 All students and staff should be aware of the risks in downloading these images as well as posting them online and sharing them with others. There are particular risks where personal images are posted onto social networking sites, for example, and these should be discussed within tutorial/lessons. The aim is to reinforce good practice as well as offer further information for all users on how to keep their personal information safe.

7.3 No image/photograph can be copied, downloaded, shared or distributed online without permission from the relevant staff or student. Photographs of activities on the College premises should be considered carefully and have the consent of the Marketing Manager before being published. If the person is identifiable, written consent should be sought.

8. Communication with students

8.3 All digital communications with students must be carried out in line with the College communications policies and be professional in tone and content at all times.

8.4 Online communication with students is restricted and must only be done through the College network or the VLE e.g. Moodle. Social networking sites should not be used by staff to make contact with students except in exceptional circumstances (e.g. gathering evidence for a cyber-bullying incident) and only then with prior written permission from the E-Safety Officer. (See ICT Acceptable Use for Staff Policy, Appendix 1 on Social Media).

9. Personal Information

9.1 Personal information is information about a particular living person. St Brendan's College collects and stores the personal information of students and staff regularly e.g. names, dates of birth, email addresses, assessment materials and so on. The College will keep that information safe and secure, and will work within the Data Protection guidance contained in the Information, Communication and Data Technology Policy.

9.2 Employment references (for staff only) will only be completed where an employee confirms they wish the College to provide a reference to a specific external organisation. The College is legally obliged to disclose information regarding disciplinary action taken against an employee, also where there are concerns in relation to Safeguarding, including E-Safety. The College will not disclose information in relation to sick absence or attendance asked on an employment reference.

9.3 No personal information can be posted to the College website without the permission of the Marketing Manager. Only names and work email addresses of some relevant staff will appear on the College website.

9.4 Staff must keep students' personal information safe and secure at all times. When using an online platform, all personal information must be password protected. No personal information of individuals is permitted offsite unless the member of staff has the permission of the E-Safety Officer or Marketing Manager.

9.5 Every user of IT facilities is required to lock or log off on completion of any activity, or where they are physically absent from a device (e.g. desktop PC). Any College mobile device (such as laptop) requires to be password protected and signed out by the relevant staff.

9.6 Where the personal data is no longer required, it must be securely deleted in line with the Data Protection Policy.

10. Education and Training.

10.1 With the current unlimited nature of internet access, it is impossible for the College to eliminate all risks for staff and students. It is our view therefore, that the College should support staff and students through training and education. This will provide them with the skills to be able to identify risks independently and manage them effectively.

10.2 For students:

Students will participate in E-safety sessions as part of their induction and tutorial programme. Issues associated with E-Safety apply across the curriculum and students should also receive guidance on what precautions and safeguards are appropriate in any subject area when making use of the internet and technologies.

Students should know what to do and who to talk to where they have concerns about inappropriate content, either where material is directed to them, or where it is discovered as part of a random search. All the College's policies relating to ICT and specific E-Safety tips and guidance will be available on Moodle and on posters around the College.

Within classes, students will be encouraged to question the validity and reliability of materials researched, viewed or downloaded. They will also be encouraged to respect the copyright of other parties and to cite references properly. Specific sessions on Information Skills such as avoiding plagiarism, using online search facilities, copyright etc. will be developed and delivered by the Learning Resource Centre.

10.3 For staff:

Staff will take part in E-Safety training and briefings, usually as part of their induction training or at the beginning of the new College year, which will be led by the E-Safety Officer. Further resources, useful guidance and information will be issued to all staff following the session. Any new or temporary staff will be asked to read and sign the Acceptable Use of ICT Policy for Staff.

11. Incidents and Response

11.1 Where an E-Safety incident is reported to the College, it will be dealt with very seriously. The College will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring. If a student wishes to report an incident, they can do so to their Pastoral Support Assistant or to the College E-Safety Officer.

11.2 Where a member of staff wishes to report an incident, they must contact their line manager. Following any incident, the College will review what has happened and decide on the most appropriate and proportionate course of action. Sanctions may be put in place, external agencies may be involved or the matter may be resolved internally depending on the seriousness of the incident.

12. Feedback

12.1 The College welcomes all constructive feedback on this Policy. If you would like further information on E-Safety, or wish to send us your comments on our E-Safety Policy, then please contact the Assistant Principal.

13. Useful Links for Further Information:

Child Exploitation & Online Protection Centre www.ceop.police.uk

Internet Watch Foundation http://mobile.iwf.org.uk

DirectGov 'Staying Safe Online'

www.direct.gov.uk/en/YoungPeople/CrimeAndJustice/KeepingSafe/DG_10027670

Get Safe Online http://www.getsafeonline.org

St Brendan's Policies:

Safeguarding Policy

Preventing Bullying and Harassment Policy

Information, Communication and Data Technology Policy (incorporating Data Protection Policy)

Acceptable Use of ICT Policies for Staff (incorporating Acceptable Use of Social Media) and the Acceptable Use of ICT Policy for Students