BILBOROUGH
SIXTH FORM COLLEGE

E-SAFETY POLICY

Update:	September 2014
Reviewed:	2 years
Lead Responsible:	Karen Lowe/Michelle Harvey

A FUTURE LESS ORDINARY

e-Safety Policy

1. Introduction

This e-safety policy should be read in conjunction with other relevant college policies to which it refers e.g. Safeguarding Policy, ICT Acceptable Use Policy, ICT Security Policy, e-Security, Anti Bullying and Disciplinary Policy.

Bilborough College recognises the benefits and opportunities which new technologies offer to teaching and learning. We provide internet access to all learners and staff and encourage the use of technologies in order to enhance skills, promote achievement and enable lifelong learning. However, the accessibility and global nature of the internet and different technologies available mean that we are also aware of potential risks and challenges associated with such use. Our approach is to implement appropriate safeguards within the college while supporting staff and learners to identify and manage risks independently and with confidence. We believe this can be achieved through a combination of security measures, training, guidance and implementation of our policies. In furtherance of our duty to safeguard learners and the Every Child Matters agenda, we will do all that we can to make our learners and staff stay e-safe and to satisfy our wider duty of care.

2. Creation, Monitoring and Review

The e-Safety Group is part of the Cross College Working Group, with responsibility for health and welfare (Safeguarding Policy, p4).

The impact of the e-Safety Policy will be monitored regularly with a full review being carried out at least once a year by the Cross College Working Group. The policy will also be reconsidered where particular concerns are raised or where an e-safety incident has been recorded.

3. Policy Scope

The e-Safety Policy applies to all users/all learners and staff/all members of the college community who have access to the college IT systems, whether on the premises or remotely. All users of college IT systems must agree to the ICT Acceptable Use Policy; which includes the e-Safety policy statements, each time they logon to the college network. The e-Safety Policy applies to all use of the internet and forms of electronic communication such as email, mobile phone, social media sites and use of images/video of the college community.

4. Roles and Responsibilities

There are clear lines of responsibility for e-safety within the college. The first point of contact should be Michelle Harvey or Madeleine Varley, the Safeguarding Offices, available in Student Support. All staff are responsible for ensuring the safety of learners and should report any concerns immediately to their line manager. All teaching staff are required to deliver e-safety guidance when using online technology in the classroom and to read through and adhere to the e-safety incident reporting procedure as contained in appendix 2. Within classes,

learners 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.

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.

All learners must know what to do if they have e-safety concerns and who to talk to. In most cases, this will be the Safeguarding Officers, Michelle Harvey or Madeleine Varley in Student Support. 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 management considers it appropriate, additional support from external agencies may be required.

The e-Safety (Safeguarding) Officer is responsible for keeping up to date with new technologies and their use, as well as attending relevant training. They will be expected to lead the e-Safety Group, complete, review and update the e-Safety Policy, deliver staff development and training, record incidents, report any developments and incidents to Karen Lowe; Assistant Principal Guidance and Support, and liaise with the local authority and external agencies to promote e-safety within the college community.

Staff will take part in Safeguarding training during the college's inset. Each member of staff must record the date of the training attended on their CPD calendar.

Any new or temporary users will receive a new password or temporary password and will be required to accept and agree to the college ICT Acceptable Use Policy, each time they logon to the college network.

All staff are responsible for using college IT systems and mobile devices in accordance with the college's ICT Acceptable Use Policy and the e-Safety Policy Statements, which they must agree to each time they logon to the college network. Staff are responsible for attending staff training on e-safety and displaying a model example to learners at all times through good practice.

All digital communications with learners must be professional at all times and be carried out in line with the college Safeguarding Policy. Online communication with learners is restricted to the college network. External platforms not hosted by the college, such as social media sites, may only be used when they are linked directly to a curriculum area for educational purposes e.g. Twitter, Facebook and should not be used for the promotion of materials or personal use.

This policy will, however, be monitored and kept under review, by the Cross College Working Group, with responsibility for health and welfare (Safeguarding Policy, p4).

Learners:

Learners are responsible for using the college IT systems and mobile devices in accordance with the college ICT Acceptable Use Policy and e-Safety Policy Statements, which they agree to each time they logon to the college system.

Learners must act safely and responsibly at all times when using the internet and/or mobile technologies. They are expected to know and act in line with other relevant college policy. They must follow reporting 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.

5. Security

The college will do all that it can to make sure 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 Security Policy; available on the college intranet, under Policies and Procedures.

6. Behaviour

Bilborough College will ensure that all users of technologies adhere to the standard of behaviour as set out in the ICT Acceptable Use Policy, which they agree to each time they logon to the college network. The college will not tolerate any abuse of IT systems. Whether offline or online, communications by staff and learners should be courteous and respectful at all times. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the student and staff disciplinary codes and Anti Bullying Policy.

Where conduct is found to be unacceptable, the college will deal with the matter internally. Where conduct is considered illegal, the college will report the matter to the police. The flowchart at appendix 2 makes it clear what sanctions will be applied for specific behaviours.

7. Use of Images and Video

The use of images, or photographs, is popular in teaching and learning and should be encouraged where there is no breach of copyright or other rights of another person (e.g. images rights or rights associated with personal data). This will include images downloaded from the internet and those belonging to staff or learners.

All learners and staff receive training on the risks when taking, downloading and posting images online and making them available to others. There are particular risks where personal images of themselves or others are posted onto social networking site. For the learner this is embedded in to the tutorial programme and during inset for staff.

Bilborough College teaching staff will provide information to learners on the appropriate use of images. . This includes photographs of learners and staff as well as using third party images. Our aim is to reinforce good practice as well as offer further information for all users on how to keep their personal information safe.

Use of photographs of activities on the college premises should be considered carefully. Learners sign a consent form during the application process, either allowing or withdrawing consent for the college's use of a learner's image. Approved photographs should not include names of individuals without consent.

8. Incidents and Response

Where an e-safety incident is reported to the college this matter 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 learner wishes to report an incident, they can do so to their personal tutor or to the college Safeguarding Officers. Where a member of staff wishes to report an incident, they must contact Michelle Harvey or Madeleine Varley without delay. 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. The e-safety incident reporting procedure flowchart in appendix 2 lists behaviours and their consequences. This is in line with the college's ICT Acceptable Use Policy. Serious incidents will be dealt with by senior management, in consultation with appropriate external agencies.

Appendix 1

E-SAFETY
POLICY STATEMENTS

✓ I will not visit sites which contain items that are illegal, defamatory, pornographic or in any way offensive.

✓ I will observe the rules and laws regarding copyright and plagiarism.

✓ I will not download files to any college computer.

✓ I will observe the requirements of the Data Protection Act 1998 and take appropriate steps to protect all personal data.

✓ I will report any information that I come across which makes me feel uncomfortable or unsafe to my Personal Tutor or a Safeguarding Officer.

✓ I agree never to write or send malicious or offensive e-mails and accept that offenders will be reported to, a Safeguarding Officer or the Assistant Principal of Guidance and Support; depending on the severity of the incident

✓ I understand that downloading and/or distributing offensive/illegal materials will lead to exclusion and possibly the involvement of the police.

✓ I agree to use photographs and video clips only with the specific permission of staff and students and only for educational purposes.

✓ I understand that if I am found to be involved in on-line bullying, that this will be dealt with in line with the college's bullying policy.

✓ I will never give my log in details to anyone else or attempt to access the network using a log in that is not my own.

✓ I will never slander staff, students or the college on a social networking site, e.g. Facebook, Twitter, Snapchat etc.

Appendix 2 - e-Safety Incident Reporting Procedures