Broadoak

College

Mathematics &

Computing

"Maximising students' abilities, ambitions and academic potential"

E-Safety Policy

Recommended by: Staff and Student Committee	
Date: January 2017	
Approved by the Full Governing Body	
Signed:	
Next review due: January 2018	

Broadoak Mathematics and Computing College is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

Purpose

This policy applies to all members of the Broadoak Mathematics and Computing College community (including staff, governors, students, volunteers, parents/carers, visitors and community users) both in and/or out of College. It is a statement of the aims, principles, strategies and procedures for e-safety throughout the College.

E-Safety refers to safeguarding of both children and adults in the digital world. It is about learning to understand and use technologies in a safe, positive way and about supporting children and adults to develop safe online behaviours.

E-Safety is largely concerned with internet communications. The internet is accessible from computers, laptops, tablets, mobile phones, and other devices like the games consoles. Other communication technologies such as texting and phone calls are also covered by the term 'E-Safety'.

The purpose of this policy is to provide the framework to nurture a safe digital community. 'Information Governance' refers to and encompasses the policies, procedures, processes and controls implemented to manage information. These support the College's immediate and future regulatory, legal, risk and operational requirements.

The following legislation and guidance must be considered when adhering to this policy:

- Obscene Publications Act 1959
- Protection of Children Act 1988
- Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- Defamation Act 1996
- Protection from Harassment Act 1997
- Human Rights Act 1998
- Data Protection Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act (RIPA) 2000
- Safeguarding Vulnerable Groups Act 2006
- Equality Act 2010
- Keeping Children Safe in Education 2016

Please note this list is intended to be indicative only

1. Managing Internet Access

- Students are required to return a signed copy of the ICT Acceptable Usage Agreement for Students which must be countersigned by their parent or carer
- All staff must read and sign the ICT Acceptable Usage Agreement for Staff and Community Users before using any College ICT resources
- College internet access will be filtered to ensure safe access to the Internet; filtering is provided by SWGfL
- The College will work in partnership with the LA, DfE and the Internet Service Provider (South West Grid for Learning) to ensure systems to protect students are reviewed and improved

- If staff or students discover an unsuitable site whilst using the College internet, the URL, content, user who made the discovery, time it was discovered and device that was being used must be reported to the IT Support who will record this in the incident report log.
- The College will ensure that use of internet derived materials by staff and students complies with copyright law.
- Logs of internet activity will be regularly checked.
- Student and staff files stored on school computers will be regularly checked.
- Student and staff emails will be regularly checked.
- Student and staff use of social networking websites will be regularly checked.
- Illegal and/or inappropriate misuse will be dealt with in accordance with the College Behaviour Policy (students) and the Staff Disciplinary Policy.

2. Use of Email

2.1 Student Use

- Students may only use official College email accounts on the College system. Personal email accounts are not to be used.
- Students must inform a member of staff if they receive an offensive or inappropriate email
- Students must not reveal personal details of themselves or others in email communication (such as address or telephone number).
- Students must not arrange to meet anyone without specific permission (e.g. for Work Experience placements in Y10).
- The forwarding of chain letters is not permitted.

2.2 Staff Use

- Personal email accounts must not be used for communication between staff and students and/or parent/carers
- Staff will sign the ICT Acceptable Usage Agreement annually and adhere to guidelines in *Guidance for Safer Working Practices for Adults working with Children and Young People*, as well as the Professional Behaviour for Staff Policy (Code of Conduct)

2.3 Parent/Carer Use

- Emails sent to Broadoak staff will be appropriate in their tone and content

3. Use of social media

3.1 Staff should ensure that:

- No reference is made in their personal use of social media about students /parents / carers or College staff.
- They do not engage in online discussion on personal matters relating to the College or members of the College community.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- Raise any concerns that any colleague(s) is/are not acting in accordance with this Policy with the Headteacher.
- Use their professional judgment and, where no specific guidance exists, take the most prudent action possible and consult with the Headteacher if they are unsure.

- Any social media accounts established for a professional purpose will be authorised by the Headteacher. These accounts must be 'public' and followed by a main Broadoak account.

3.2 Students should ensure that:

- No images of staff, students or visitors to the College are posted online without their consent.
- They understand the Behaviour and Anti Bullying Policies apply to their use of social media and that sanctions could be applied if they use social media inappropriately.

4. Mobiles, cameras and portable digital devices

4.1 Students

- Mobile phones, tablets, portable electronic games and media players should not be used during lessons, unless given permission to do so by a member of staff.
- The sending of abusive or inappropriate text messages could result in sanctions, in line with the College's Behaviour and Anti Bullying Policies.
- Inappropriate use of mobile technology could result in the items being confiscated, in line with the Mobile Phone Protocol.

4.2 Staff:

- Use of personal mobile phones in school must be within the ICT Acceptable Usage Agreement.
- Staff must not keep or use personal mobile phones in view of students.
- Staff must not use personal mobile phones in the vicinity of students (e.g. if there are students in the staff room or offices).
- Staff must not use personal devices to take images of students.
- Staff must not use personal devices to take any images, video or sound recordings in College.
- Staff are allowed to take digital photographs and video images to support educational aims, but follow guidance in the ICT Acceptable Usage Agreement for Staff and Community Users concerning the taking, sharing, distribution and publication of those images.
- Text messaging must not be used for communication between staff and parents/carers other than through the Schoolcomms system.
- Staff who are issued with laptops must sign the appropriate agreement.

4.3 Visitors to the College (including parents/carers)

- Visitors must not use personal devices to take images of students.
- Visitors must not use personal devices to take any images, video or sound recordings in College.
- Any photos taken must be for promotional or educational purposes only and should have permission to be taken by supervising staff.

5. Memory Sticks and other portable storage

This includes portable USB flash drives and portable hard disk drives. The Information Commissioner's Office has the power to impose hefty fines on schools <u>and individuals</u> who lose personal data. The loss of an unencrypted memory stick containing the names of students would count. The school's Data Protection Policy applies in these cases. Staff should only use encrypted memory sticks for storing information.

6. College Website

- The point of contact on the website should be the College address, email and telephone number. Staff or students' personal information will not be published.
- Website photographs that include students will be selected carefully and will only be published with parental permission.
- Students' full names will not be used anywhere on the website, particularly in association with photographs.

7. Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment carried out before use in school is allowed.

8. Teaching and Learning

Whilst regulation and technical solutions are very important, their use must be balanced with educating learners to take a responsible approach. The education of students in e-safety is therefore an essential part of the school's e-safety provision. Students need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

- There are planned e-safety lessons delivered through Computing and PSHCE.
- Key e-safety messages are reinforced through assemblies and tutor time activities.
- In lessons where internet use is pre-planned, students are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, e.g. using search engines, staff are vigilant in monitoring the content of the websites the young people visit and encourage students to use specific search terms to reduce the likelihood of coming across unsuitable material.
- Students are taught to be critically aware of the materials / content they access online and be guided to validate the accuracy of information.
- When using digital images, Students are taught about the risks associated with the taking, use, sharing, publication and distribution of images including on social networking sites
- Staff act as good role models in their own use of ICT.
- Staff are familiar with and ensure that Students act in accordance with the ICT Acceptable Usage Agreement for Students.

9. Role of parents and carers

Parents and carers may have only a limited understanding of e-safety issues and may be unaware of risks and what to do about them. However, they have a critical role to play in supporting their children with managing e-safety risks at home, reinforcing key messages about e-safety and regulating their home experiences. The College will support parents/carers to do this by providing regular newsletter and website updates on e-safety.

Parents and carers also have a responsibility to act as positive role models for their children in their use of ICT/social media.

Linked Policies

- Behaviour Policy
- Anti-Bullying Policy
- CCTV Policy
- Data Protection Policy
- Code of Conduct
- Whistleblowing Policy
- Staff Disciplinary Policy
- Mobile Phone Protocol