Online Safety Policy

Date of Publication	**January 2022**
Date of Next Review	**January 2023**
Senior Designated Safeguarding Person (SDSP)	**Anne Entwistle/Nadia Khan**
Designated Safeguarding Person (DSP)	**Alex Pazik**
Nominated Safeguarding Governor	**Signe Sutherland**
Policy Creator	**Alex Pazik**
Approved by	**Anne Entwistle**

This policy should be interpreted in the context of other relevant College Policies and Procedures, particularly BCA Safeguarding Child Protection and Safeguarding Policy (January 2022), BCA Safeguarding Annual Audit December (April 2021) and the Single Equality Scheme (Oct 2022).

This document can be made available in other formats, on request

Purpose

Providing high quality education that gives our students the knowledge, skills and experience to be successful in their chosen career.

BCA Equality and Diversity Ethos Statement

This policy and procedure is subject to The Equality Act 2010 which recognises the following categories of individual as Protected Characteristics: Age, Gender Reassignment, Marriage and Civil Partnership, Pregnancy and Maternity, Race, Religion and Belief, Sex (gender), Sexual orientation, Disability, Socio-economic Disadvantage

This policy is designed to safeguard our young people, vulnerable adult learners and staff.

BCA recognises that ICT and the Internet are fantastic tools for learning and communication that can be used in college to enhance the curriculum, challenge students, and support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone in the college community, but it is important that the use of the Internet and ICT 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 college community are aware of the dangers of using the Internet and know how they should conduct themselves online.

Online safety covers the Internet but it also covers mobile phones and other electronic communications technologies. We know that some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings. There is a 'duty of care' for any persons working with children and educating all members of the college community on the risks and responsibilities of online safety falls under this duty. It is important that there is a balance between controlling access to the Internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating ICT activity in college, and provide a good understanding of appropriate ICT use that members of the college community can use as a reference for their conduct online outside of college hours. Online safety is a whole-college issue and responsibility.

1. **Roles and Responsibilities**

Principal and SLT

The Principal has a duty of care for ensuring the safety (including online safety) of members of the college community, though the day-to-day responsibility for online safety will be delegated to the SDSL/DSLs. Any complaint about staff misuse must be referred to the SDSL/DSL at the college or, in the case of a serious complaint, to the Principal.

● Ensure access to induction and training in online safety practices for all users.

● Ensure appropriate action is taken in all cases of misuse.

● Ensure that Internet filtering methods are appropriate, effective and reasonable.

● Ensure that staff or external providers who operate monitoring procedures be supervised by a named member of SLT.

● Ensure that student or staff personal data as recorded within college management system sent over the Internet is secured.

● Work in partnership with the DFE and the Internet Service Provider and college ICT Manager to ensure systems to protect students are reviewed and improved.

● Ensure the college ICT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly.

● SDSL/DSL will receive daily monitoring reports from the online safety filters (Smoothwall) and in serious breaches of online use an instant report will be sent via Smoothwall.

ICT Manager/Technical Staff:

The ICT Manager is responsible for ensuring:

● That the college's technical infrastructure is secure and is not open to misuse or malicious attack.

● That the college 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 policy.

● The filtering policy is applied and updated on a regular basis.

● That they keep up to date with online safety technical information in order to effectively carry out their role and to inform and update others as relevant.

● That the use of the network/internet/Virtual Learning Environment/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Principal; SDSL/DSLs for investigation/action/sanction

● That monitoring software/systems are implemented and updated as required

2. **Communicating College Policy**

This policy is available on the staff hand book and college website for parents, staff, and students to access as and when they wish. Rules relating to the college code of conduct when online, and e-safety guidelines, are discussed during student enrolment and induction. Online safety is integrated into the curriculum in any circumstance where the Internet or technology are being used.

3. **Making use of ICT and the Internet in college**

The Internet is used in college to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the college's management systems. Technology is advancing rapidly and is now a huge part of everyday life, education and business. We want to equip our students with all the necessary ICT skills that they will need in order to enable them to progress confidently into a professional working environment when they leave college.

Some of the benefits of using ICT and the Internet in college are:

For students:

- Unlimited access to worldwide educational resources and institutions such as art galleries, museums and libraries.
- An enhanced curriculum; interactive learning tools; collaboration, locally, nationally, and globally; self-evaluation; feedback and assessment; updates on current affairs as they happen.
- Access to learning whenever and wherever convenient.
- Freedom to be creative.
- Freedom to explore the world and its cultures from within a classroom.
- Social inclusion, in class and online.
- Access to case studies, videos and interactive media to enhance understanding.
- Individualised access to learning.

For staff:

- Professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies.
- Immediate professional and personal support through networks and associations.
- Improved access to technical support.
- Ability to provide immediate feedback to students and parents.
- Class management, attendance records, schedule, and assignment tracking.

4. **Managing Information Systems**

The college is responsible for reviewing and managing the security of the computers and Internet networks as a whole and takes the protection of college data and personal protection of our college community very seriously. This means protecting the college network, as far as is practicably possible, against viruses, hackers and other external security threats. The IT Technicians/ICT Manager will review the security of the college information systems and users regularly and virus protection software will be updated regularly. Some safeguards that the college takes to secure our computer systems are:

- Ensuring that all personal data sent over the Internet or taken off site is encrypted
- Making sure that unapproved software is not downloaded to any college computers. Alerts will be set up to warn users of this
- Files held on the college network will be regularly checked for viruses
- The use of user logins and passwords to access the college network will be enforced
- Portable media containing college data or programmes will not be taken off-site without specific permission from *a member of the senior leadership team.*

5. **Emails**

The college uses email internally for staff and students, and externally for contacting parents and other professionals, and is an essential part of college communication.

Staff and students should be aware that college email accounts should only be used for college-related matters, ie for staff to contact parents, students, other members of staff and other professionals for work purposes. This is important for confidentiality. The college has the right to monitor emails and their contents but will only do so if it feels there is reason to.

6. **College Email Accounts and Appropriate Use**

Staff should be aware of the following when using email in college:

- Staff should only use official college-provided email accounts to communicate with students, parents or carers. Personal email accounts should not be used to contact any of these people.
- Emails sent from college accounts should be professionally and carefully written. Staff are representing the college at all times and should take this into account when entering into any email communications.
- Staff must tell their manager or a member of the senior leadership team if they receive any offensive, threatening or unsuitable emails either from within the college or from an external account. They should not attempt to deal with this themselves.

Students should be aware of the following when using email in college, and will be taught to follow these guidelines through the ICT curriculum and in any instance where email is being used within the curriculum or in class:

- Students should tell a member of staff if they receive any offensive, threatening or unsuitable emails either from within the college or from an external account. They should not attempt to deal with this themselves.
- Students must be careful not to reveal any personal information over email, or arrange to meet up with anyone who they have met online without specific permission from an adult in charge.

Students will be educated to identify spam, phishing and virus emails and attachments that could cause harm to the college network or their personal account or wellbeing.

7. **Published Content and the College Website**

The college website is viewed as a useful tool for communicating our college ethos and practice to the wider community. It is also a valuable resource for parents, students, and staff for keeping up-to-date with college news and events.

The website is in the public domain, and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the college community, copyrights and privacy policies. No personal information on staff or students will be published.

8. **Social Networking, Social Media and Personal Publishing**

Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging programmes. These online forums are the more obvious sources of inappropriate and harmful behaviour and where students are most vulnerable to being contacted by a dangerous person. It is important that we educate students so that they can make their own informed decisions and take responsibility for their conduct online.

Social media sites have many benefits for both personal use and professional learning; however, both staff and students should be aware of how they present themselves online. Students are taught about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place. The college follows general rules on the use of social media and social networking sites in college:

- Students are educated on the dangers of social networking sites and how to use them in safe and productive ways. They are all made fully aware of the college's code of conduct regarding the use of ICT and technologies and behaviour online.
- Students and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The college expects all staff and

students to remember that they are representing the college at all times and must act appropriately.

- Safe and professional behaviour of staff online is discussed at staff induction.

9. **Mobile Phones and Personal Device**

While mobile phones and personal communication devices are commonplace in today's society, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are they:

- Can make students and staff more vulnerable to cyber bullying
- Can be used to access inappropriate internet material
- Can be a distraction in the classroom
- Are valuable items that could be stolen, damaged, or lost
- Can have integrated cameras, which can lead to child protection, bullying and data protection issues.

The college takes certain measures to ensure that mobile phones are used responsibly in college. Some of these are outlined below.

- The college will not tolerate cyber bullying against either students or staff. Sending inappropriate, suggestive or abusive messages is forbidden and anyone who is found to have sent a message of such content will be disciplined. For more information on the college's disciplinary procedures read the **student code of conduct.**
- Mobile phones must be switched off during lessons or any other formal college activities unless being used for a learning purpose.
- Any student who brings a mobile phone or personal device into college is agreeing that they are responsible for its safety. The college will not take responsibility for personal devices that have been lost, stolen, or damaged.
- Images or files should not be sent between mobile phones in college.

Mobile Phone or Personal Device Misuse

Students

- Students who breach college policy relating to the use of personal devices will be disciplined in line with the student code of conduct.
- Students are under no circumstances allowed to bring mobile phones or personal devices into examination rooms with them. If a student is found with a mobile phone in their possession it will be confiscated. The breach of rules will be reported to the appropriate examining body and may result in the students being prohibited from taking that exam.

Staff

- Under no circumstances should staff use their own personal devices to contact students or parents either in or out of college time.
- Staff are not permitted to take photos or videos of students. If photos or videos are being taken as part of the college curriculum or for a professional capacity, the college equipment will be used for this.
- The college expects staff to lead by example. Personal mobile phones should be used at a minimum.
- Any breach of college policy may result in disciplinary action against that member of staff.

10. **Cyberbullying**

The college, as with any other form of bullying, takes Cyber bullying, very seriously**.** Cyber-bullying by students will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures (see BCA Bullying 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 college 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 college will:

- Take it seriously
- Act as quickly as possible to establish the facts. It may be necessary to examine college 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. It is important that young people or vulnerable adults who have harmed another, either physically or emotionally, redress their actions and the college 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. The police may be required to be contacted.

11. **Protecting Personal Data**

BCA believes that protecting the privacy of our staff and students and regulating their safety through data management, control and evaluation is vital to whole-college and individual progress. The college collects personal data from students, parents, and staff and processes it in order to support teaching and learning, monitor and report on student and teacher progress, and strengthen our pastoral provision.

We take responsibility for ensuring that any data that we collect and process is used correctly and only as is necessary. Through effective data management we can monitor a range of college provisions and evaluate the wellbeing and academic progression of our college body to ensure that we are doing all we can to support both staff and students.

In line with the Data Protection Act 1998, and following principles of good practice when processing data, the college 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 college is required either by law or in the best interests of our students or staff to pass information onto external authorities; for example, our local authority, Ofsted, 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.