ICT E-Safety Policy

Content Page

Brighton Forward is committed to reviewing its policy and good practice annually.

This policy was revised on 20th January 2025

Laura Vallone

Introduction
At Brighton Forward we believe that ICT is central to all aspects of learning, for adults and students in both the college and wider community. Provision should reflect the rapid developments in technology.

ICT in the 21st Century is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of young people and adults. Consequently, we need to build in the use of these technologies in order to equip our young people with the skills to access lifelong learning and employment.

All students, whatever their needs, will have access to a range of up-to-date technologies during sessions. ICT is a life skill and should not be taught in isolation.

It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies students will use both inside and outside of the college include:

• Websites
• Learning Platforms and Virtual Learning Environments
• Email and Instant Messaging
• Chat Rooms and Social Networking
• Blogs
• Podcasting
• Video Broadcasting
• Music Downloading
• Gaming
• Mobile/ Smart phones with text, video and/ or web functionality
• Other mobile devices with web functionality

All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Brighton Forward, we understand the responsibility to educate our students on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies.

We know that it is not sufficient enough to ban or block inappropriate sites, so our aim is to educate students by giving them the skills and knowledge they need to use technology safely and responsibly. As well as the benefits to using technology, there are risks and our students need to be able to manage these.

Whole college approach
All members of the college community have a responsibility for promoting and supporting safe behaviours and follow college e-safety procedures. This includes vigilance when students are accessing the internet at college to ensure that they do not access inappropriate websites.

All staff should be familiar with the college's policy including:

- safe use of e-mail
- safe use of the Internet
- safe use of the college network, equipment and data
- safe use of digital images and digital technologies, such as mobile phones and digital cameras
- publication of student information/photographs on the school website

- procedures in the event of misuse of technology by any member of the college community (see appendices)
- their role in providing e-safety education for students

Staff are reminded/updated about e-safety regularly and new staff and students receive information on the college's Acceptable Use Policy as part of their induction.

E-safety in the programme
We provide opportunities to teach about e-safety by:

- Educating students on the dangers of technologies that may be encountered outside college is done informally when opportunities arise and as part of the curriculum
- Students are taught about copyright and respecting other people's information, images, etc. through discussion, modelling, and activities as part of Personal Development and IT sessions
- Students are aware of the impact of online bullying through Personal Development and are taught how to seek help if they are affected by these issues. Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies (cyber bullying)
- Students are taught to critically evaluate materials and learn good searching skills
- Students are taught about the risks inherent in using social media, particularly if they are contacted by people they do not know

Managing Internet Access
Students will have supervised access to Internet resources

- Staff must preview any recommended sites before use. Particular care must be taken when using search engines with the students as these can return undesirable links.
- Staff and students are aware that college based email and internet activity can be monitored and explored further if required.
- If staff or students discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to a member of the senior management.
- It is the responsibility of the college to ensure that antivirus protection is installed and kept up-to-date on all college machines.

E-mail
The use of email within college is an essential means of communication for staff. In the context of college, email should not be considered private. Educationally, email can offer significant communication advantages and we recognise that students need to understand how to style an email in relation to their age.

- Students are introduced to email as part of IT
- The college gives staff their own email account, to use for all college business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- Under no circumstances should staff contact students or parents using personal email addresses.
- Students may only use college approved accounts on the college system and only under direct facilitator supervision for educational purposes.
- The forwarding of chain letters is prohibited in college.

- Students must immediately tell a facilitator / trusted adult if they receive an offensive e-mail. All students must use appropriate language in e-mails and must not reveal personal details of themselves or others in e-mail communication or arrange to meet anyone. Staff must inform a member of SLT if they receive an offensive e-mail.

Publishing student's images and work

On application to Brighton Forward, all parents/carers will be asked to give permission for their child's photo to be taken and to use their child's work/photos in the following ways:

- On the college web site
- In display material that may be used in the college's communal areas
- In display material that may be used in external areas, i.e. exhibition promoting the college
- General media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically.)

Students' names will not be published alongside their image and vice versa without permission from the parents/carers. Full names will not be published.

Social networking and personal publishing

We support students in the appropriate use of social networking sites. Students and parents will be advised that the use of social network spaces outside college should be monitored by the home.

Students will be advised never to give out personal details of any kind which may identify them or their location.

Data protection

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

This policy sets out the manner in which personal data of staff, students and other individuals is processed fairly and lawfully.

The college collects and uses personal information about staff, students, parents or carers and other individuals who come into contact with the college. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the college complies with its statutory obligations.

The college is a data controller and must therefore comply with the Data Protection Principles in the processing of personal data, including the way in which the data is obtained, stored, used, disclosed and destroyed.

Responding to e-safety incidents/complaints

As a college we will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a college computer or mobile device. The college cannot accept liability for material accessed, or any consequences of Internet access. Complaints relating to e-safety should be made to a member of the senior leadership team. Any complaint about staff misuse must be referred to the Managing Director.

- All users are aware of the procedures for reporting accidental access to inappropriate materials. Any breach must be immediately reported.

- Deliberate access to inappropriate materials by any user will lead to the incident being logged and, depending on the seriousness of the offence; investigation by the Managing Director, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences
- Students and parents will be informed of the complaints procedure.
- Parents and students will need to work in partnership with staff to resolve issues.

Cyberbullying
Cyberbullying is the use of ICT, particularly mobile phones and the internet, to deliberately upset someone else. The whole college community has a duty to protect all its members and provide a safe, healthy environment.

Although bullying is not a specific criminal offence in the UK law, there are laws that can apply in terms of harassing or threatening behaviour, for example, or indeed menacing and threatening communications.

Preventing Cyberbullying
It is important that we work in partnership with students and parents to educate them about Cyberbullying as part of our e-safety curriculum.

They should:
- understand how to use these technologies safely and know about the risks and consequences of misusing them
- know what to do if they or someone they know are being cyber bullied.
- report any problems with Cyberbullying. If they do have a problem, they can talk to the college, parents, the police, the mobile network (for phone) or the Internet Service Provider (ISP) to do something about it.

Additional online advice on how to react to Cyberbullying can be found on www.kidscape.org and www.wiredsafety.org

Supporting the person being bullied
Support shall be given in line with the behaviour policy:
- Give reassurance that the person has done the right thing by telling someone and inform parents.
- Make sure the person knows not to retaliate or return the message.
- Help the person keep relevant evidence for any investigation (taking screen capture shots, not deleting messages.)
- Check the person knows how to prevent it from happening again e.g. blocking contacts, changing contact details.
- Take action to contain the incident when content has been circulated: remove content, contact the host (social networking site) to get the content taken down, use disciplinary powers to confiscate phones that are being used to cyber bully – ask the student who they have sent messages to.

Investigating Incidents
All bullying incidents should be recorded and investigated in the incident log as any other bullying incident. We will then investigate fully as any other bullying incident (refer to behaviour policy).

Working in Partnership with Parents
Parents/carers are asked to read through and sign acceptable use of ICT agreement along with the student.
- A partnership approach with parents will be encouraged including suggestions for safe home Internet use.

- Advice on filtering systems and educational activities that include safe use of the Internet will be made available to parents.

Reviewing this Policy

There will be an on-going opportunity for staff to discuss with SLT any issue of safety that concerns them.

This policy will be reviewed every 12 months and consideration given to the implications for future whole school development planning.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.