**Brighton Forward**

**Online Safety Policy**

**Contents** **Page**



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

Reviewed by: Laura Vallone
Review date: 22nd March 2026
Next review date: March 2027

## 1. Aims

Our college aims to:

- Have robust processes in place to ensure the online safety for all students, staff and free staff.
- Identify and support groups of students that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole college community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

### The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit the user for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

## 2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for colleges on:

- Teaching online safety
- Meeting digital and technology standards https://www.gov.uk/government/publications/preventing-and-tackling-bullying
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and college staff
- **Relationships and sex education (RSE) and health education**
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate

images or files on students' electronic devices where they believe there is a 'good reason' to do so.

## 3. Roles and responsibilities

### 3.1 The Managing Director

The Managing Director has overall responsibility for monitoring this policy, holding the Programme Lead and Lead Facilitator's to account for its implementation.

The Managing Director will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around monitoring.

The Managing Director will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The Managing Director will co-ordinate regular meetings with appropriate staff to discuss online safety and requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The Managing Director will make sure that the college teaches students how to keep themselves and others safe, including online.

The Managing Director will make sure that the college has appropriate filtering and monitoring systems in place on college devices and college networks, and will regularly review their effectiveness. They will review the DfE's filtering and monitoring standards, and know what needs to be done to support the college in meeting the standards, which include:

- Reviewing monitoring provisions at least annually
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- Having effective monitoring strategies in place that meet the college's safeguarding needs

Managing Director will:

- Make sure they have read and understand this policy
- Agree and adhere to the terms on acceptable use policy
- Make sure that online safety is a running and interrelated theme when devising and implementing the whole-college or college approach to safeguarding and related policies and/or procedures
- Make sure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some students with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach is not be appropriate for all young people in all situations, and a more personalised or contextualised approach is often be more suitable

### 3.2 The Lead Facilitator

The Lead Facilitator of each site is responsible for making sure that staff understand this policy, and that it is being implemented consistently throughout the college.

### 3.3 The designated safeguarding lead (DSL)

Details of the college's designated safeguarding lead (DSL) and deputy are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in college, in particular:

- Supporting the Lead Facilitators in making sure that staff understand this policy and that it is being implemented consistently throughout the college
- Working with the Leads and Directors to review this policy annually and make sure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the monitoring systems and processes in place on college devices and college networks
- Working with the all staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the college's child protection policy
- Responding to safeguarding concerns identified by our monitoring process
- Making sure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the college behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in college to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks students face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

### 3.4 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use policy and making sure that students follow the college's terms on acceptable use
- Knowing that the DSL is responsible for the monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by emailing aine@brightonforward.co.uk
- Working with the DSL to make sure that any online safety incidents are logged and dealt with appropriately in line with this policy

- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the college behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

### 3.6 Parents/carers

Parents/carers are expected to:

- Notify a Lead Facilitator or the Managing Director of any concerns or queries regarding this policy
- Make sure that their child has read, understood and agreed to the terms on acceptable use policy
- Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:
- What are the issues? – UK Safer Internet Centre
- Help and advice for parents/carers – Childnet
- Parents and carers resource sheet – Childnet

### 3.7 Visitors and members of the community

Visitors and members of the community who use the college's ICT systems or internet will be made aware of this policy and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

## 4. Educating students about online safety

### 4.1 Students will be taught about online safety as part of the programme

Students will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns
- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of college**, students will know:

- Rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- Online risks, including the importance of being cautious about sharing personal information online and of using privacy and location settings appropriately to protect information online. Students should also understand the difference between public and private online spaces and related safety issues

- The characteristics of social media, including that some social media accounts are fake, and / or may post things which aren't real / have been created with AI. That social media users may say things in more extreme ways than they might in face-to-face situations, and that some users present highly exaggerated or idealised profiles of themselves online
- Not to provide material to others that they would not want to be distributed further and not to pass on personal material which is sent to them. Students should understand that any material provided online might be circulated, and that once this has happened there is no way of controlling where it ends up. Students should understand the serious risks of sending material to others, including the law concerning the sharing of images
- That keeping or forwarding indecent or sexual images of someone under 18 is a crime, even if the photo is of themselves or of someone who has consented, and even if the image was created by the child and/or using AI-generated imagery. Students should understand the potentially serious consequences of acquiring or generating indecent or sexual images of someone under 18, including the potential for criminal charges and severe penalties including imprisonment. Students should know how to seek support and should understand that they will not be in trouble for asking for help, either at college or with the police, if an image of themselves has been shared. Students should also understand that sharing indecent images of people over 18 without consent is a crime
- What to do and how to report when they are concerned about material that has been circulated, including personal information, images or videos, and how to manage issues online
- About the prevalence of deepfakes including videos and photos, how deepfakes can be used maliciously as well as for entertainment, the harms that can be caused by deepfakes and how to identify them
- That the internet contains inappropriate and upsetting content, some of which is illegal, including unacceptable content that encourages misogyny, violence or use of weapons. Students should be taught where to go for advice and support about something they have seen online. Students should understand that online content can present a distorted picture of the world and normalise or glamorise behaviours which are unhealthy and wrong
- That social media can lead to escalations in conflicts, how to avoid these escalations and where to go for help and advice
- How to identify when technology and social media is used as part of bullying, harassment, stalking, coercive and controlling behaviour, and other forms of abusive and/or illegal behaviour and how to seek support about concerns
- That pornography, and other online content, often presents a distorted picture of people and their sexual behaviours and can negatively affect how people behave towards sexual partners. This can affect students who see pornographic content accidentally as well as those who see it deliberately. Pornography can also portray misogynistic behaviours and attitudes which can negatively influence those who see it
- How information and data is generated, collected, shared and used online

- That websites may share personal data about their users, and information collected on their internet use, for commercial purposes (e.g. to enable targeted advertising)
- That criminals can operate online scams, for example using fake websites or emails to extort money or valuable personal information. This information can be used to the detriment of the person or wider society. About risks of sextortion, how to identify online scams relating to sex, and how to seek support if they have been scammed or involved in sextortion
- That AI chatbots are an example of how AI is rapidly developing, and that these can pose risks by creating fake intimacy or offering harmful advice. It is important to be able to critically think about new types of technology as they appear online and how they might pose a risk

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some students with SEND.

### 4.2 Students will be taught practical cyber security skills

All students will receive cogitation appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Students will also receive cogitation appropriate education on safeguarding issues such as cyberbullying and the risks of online radicalisation.

## 5. Cyber-bullying

### 5.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the college behaviour policy.)

### 5.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and encourage them to do so, including where they are a witness rather than the victim.

The college will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Facilitators will discuss cyber-bullying with students.

Facilitators are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training (see section 11 for more detail).

In relation to a specific incident of cyber-bullying, the college will follow the processes set out in the college behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, the college will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

### 5.3 Artificial intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, students and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Brighton Forward recognises that AI has many uses to help students learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone’s likeness.

Brighton Forward will treat any use of AI to bully students very seriously, in line with our anti bullying and behaviour policy.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by the college, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, students and staff.

## 6. Acceptable use of the internet in college

All students, staff, volunteers and are expected to sign an agreement regarding the acceptable use of the college’s ICT systems and the internet.

Use of the college’s internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual’s role.

## 7. Students using mobile devices in college

Students may bring mobile devices into college, but are not permitted to use them during sessions.

Any use of mobile devices in college by students must be in line with the acceptable use agreement.

Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the college behaviour policy, which may result in the confiscation of their device.

## 8. Staff using work devices outside college

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords can be made up of 3 random words, in combination with numbers and special characters if required, or generated by a password manager
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by promptly installing the latest updates

Staff members must not use the device in any way that would violate the college's terms of acceptable use.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the Lead Facilitator or DSL.

**9. How the college will respond to issues of misuse**

Where a student misuses the college's ICT systems or internet, we will follow the procedures set out in our policies for behaviour and acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the college's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures / staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The college will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

**10. Training for staff**

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
  - Abusive, threatening, harassing and misogynistic messages

- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content

› Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

› Develop better awareness to assist in spotting the signs and symptoms of online abuse

› Develop the ability to ensure students can recognise dangers and risks in online activity and can weigh up the risks

› Develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputy will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

More information about safeguarding training is set out in our child protection and safeguarding policy.

## 11. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety

This policy will be reviewed every year by the Managing Director. At every review, the policy will be shared with all staff. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks students face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

## 12. Links with other policies

This online safety policy is linked to our:

| | |
|---|---|
| Child protection and safeguarding policy | Behaviour policy |
| Staff disciplinary procedures | Data protection policy |
| Complaints procedure | Acceptable use policy |