Brixham College

Online Safety Policy

March 2021

Date adopted	March 2021
Prepared by	Richard Burden – DSL Dan Bunce - Head of ICT
Ratified by:	The Trustees
Reviewed on:	March 2023

Contents

1. Aims

Our College aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and Trustees
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole College community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for Colleges on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department'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.

The policy also takes into account the National Curriculum computing programmes of study. and KCSIE 2019.

3. Roles and responsibilities

3.1 The board of Trustees

The board of Trustees has overall responsibility for monitoring this policy and holding the Principal to account for its implementation.

The board of Trustees will co-ordinate regular meetings with appropriate staff to discuss online safety, and scrutinise information provided by the designated safeguarding lead (DSL).

All Trustees will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the College's ICT systems and the internet (appendix 2)

3.2 The Principal

The Principal is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the College.

3.3 The designated safeguarding lead

Details of the College's designated safeguarding lead (DSL) are set out in our child protection and safeguarding policy.

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

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the College
- Working with the Principal, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring 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 (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in College to the Principal and/or board of Trustees

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep students safe from potentially harmful and inappropriate content and contact online while at College, including terrorist and extremist material
- Monitor internet access by use of daily reports to ensure safeguarding checks are satisfied
- Ensuring that the College's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the College's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the College behaviour policy
- Produce scheduled reports and alerts to highlight attempts to access 'suspicious' sites.
- Providing support to Staff investigating online safety incidents and lead where appropriate
- Liaise with Police and External agencies, assisting with online investigations and evidence gathering.

This list is not intended to be exhaustive.

3.5 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 of the College's ICT systems and the internet (appendix 2), and ensuring that students follow the College's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the College behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the Principal of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the College's ICT systems and internet.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

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, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use and sign a copy of the policy before being given access to College Systems.

4. Educating students about online safety

Students will be taught about online safety as part of the curriculum.

In **Key Stage 3**, 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

Students in **Key Stage 4** will be taught:

- 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

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

The College will use assemblies, SiL lessons, FLD days and tutorial to raise students' awareness of the dangers that can be encountered online and may also invite speakers to talk to students about this.

5. Educating parents about online safety

The College will raise parents' awareness of internet safety in letters or other communications home, and in information published via our website. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Principal, DSL or by emailing esafety@brixhamcollege.co.uk.

Concerns or queries about this policy can be raised with any member of staff or the Principal.

Communication will also be made with parent and carers by email, text or Groupcall on any topical issues that may arise with advise and guidance should there be a need.

6. Cyber-bullying

6.1 Definition

Cyberbullying is bullying that takes place over digital devices like cell phones, computers, and tablets. Cyberbullying can occur through SMS, Text, and apps, or online in social media, forums, or gaming where people can view, participate in, or share content. Cyberbullying includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can include sharing personal or private information about someone else causing embarrassment or humiliation. Some cyberbullying crosses the line into unlawful or criminal behaviour.

The most common places where cyberbullying occurs are:

Social Media, such as Facebook, Instagram, Snapchat, and Twitter

SMS (Short Message Service) also known as Text Message sent through devices

Instant Message (via devices, email provider services, apps, and social media messaging features)

Email

Special Concerns

With the prevalence of social media and digital forums, comments, photos, posts, and content shared by individuals can often be viewed by strangers as well as acquaintances. The content an individual shares online – both their personal content as well as any negative, mean, or hurtful content – creates a kind of permanent public record of their views, activities, and behavior. This public record can be thought of as an online reputation, which may be accessible to Colleges, employers, colleges, clubs, and others who may be researching an individual now or in the future. Cyberbullying can harm the online reputations of everyone involved – not just the person being bullied, but those doing the bullying or participating in it. Cyberbullying has unique concerns in that it can be:

- **Persistent** – Digital devices offer an ability to immediately and continuously communicate 24 hours a day, so it can be difficult for children experiencing cyberbullying to find relief.
- **Permanent** – Most information communicated electronically is permanent and public, if not reported and removed. A negative online reputation, including for those who bully, can impact college admissions, employment, and other areas of life.
- **Hard to Notice** – Because teachers and parents may not overhear or see cyberbullying taking place, it is harder to recognise.

6.2 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 are encouraged 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. Class teachers/form tutors will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

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

The College also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

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 consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Upskirting

This refers to taking a picture under a person's clothing without them knowing, with the intention of viewing their genitals or buttocks to obtain sexual gratification or cause the victim humiliation, distress or alarm (DfE 2019). This is a criminal offence and should an incident occur a referral to the police will be made immediately.

6.4 Examining electronic devices

College staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the College rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of College discipline), and/or
- Report it to the police

Any searching of students will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the College complaints procedure.

7. Acceptable use of the internet in College

All students, parents, staff, volunteers and Trustees are expected to sign an agreement regarding the acceptable use of the College's ICT systems and the internet. Visitors will be expected to read and agree to the College's terms on acceptable use if relevant. If appropriate, they will be expected to agree to the terms on acceptable use and sign a copy of the policy before being given access to College Systems.

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.

We will monitor the websites visited by students, staff, volunteers, Trustees and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements available on the College website

8. Students using mobile devices in College

Students may bring mobile devices into College, but are only permitted to use them during:

- Social time before and after College
- Break times
- Clubs before or after College, or any other activities organised by the College at the express permission of the teacher present
- Phones and headphones should be out of sight and silent throughout lesson and transitions unless specifically given permission by staff to use them

Any use of mobile devices in College by students must be in line with the acceptable use agreement (see appendix 1).

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.

9. Staff using work devices outside College

Staff members using a work device outside College must not install any unauthorised software on the device and must not use the device in any way which would violate the College's terms of acceptable use. Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside College. Any USB devices containing data relating to the College must be encrypted and this will be enforced by system policies.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

10. 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 the behaviour policy. 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. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including social media use, 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, e-bulletins and staff meetings).

The DSL 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.

Trustees will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

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

12 . Covid Pandemic – increase in online learning

There has been a sharp increase in the use of technology for remote learning since March 2020 and the following information provides some basic guidelines for staff and school leaders

When selecting a platform for online / virtual teaching, settings should satisfy themselves that the provider has an appropriate level of security. Wherever possible, staff should use school devices and contact students only via the student school email address / log in. This ensures that the setting's filtering and monitoring software is enabled

In deciding whether to provide virtual or online learning for students, senior leaders should take into account issues such as accessibility within the family home, the mental health and wellbeing of children, including screen time, the potential for inappropriate behaviour by staff or students, staff access to the technology required, etc. Virtual lessons should be timetabled and senior staff, DSL and / or heads of department should be able to drop in to any virtual lesson at any time – the online version of entering a classroom

Staff engaging in online learning should display the same standards of dress and conduct that they would in the real world; they should also role model this to students and parents. The following points should be considered:-

- think about the background; photos, artwork, identifying features, mirrors – ideally the backing should be blurred
- staff and students should be in living / communal areas – no bedrooms
- staff and students should be fully dressed
- filters at a child's home may be set at a threshold which is different to the school
- resources / videos must be age appropriate – the child may not have support immediately to hand at home if they feel distressed or anxious about content
- Live classes should be kept to a reasonable length of time
- Language must be professional and appropriate, including any family members in the background
- Schools should risk assess the use of live learning using webcams
- Data Controllers need to reassure themselves that any teaching/learning software and/or platforms are suitable and raise no privacy issues; or use cases against the
- providers terms and conditions (for example, no business use of consumer products)

It is the responsibility of the staff member to act as a moderator; raise any issues of suitability (of dress, setting, behaviour) with the child and / or parent immediately and end the online interaction if necessary.

Recording lessons does not prevent abuse. If staff wish to record the lesson they are teaching, consideration should be given to data protection issues; e.g., whether parental / student consent is needed and retention / storage. If a staff member believes that a child or parent is recording the interaction, the lesson should be brought to an end or that child should be logged out immediately. Staff, parent and student contracts should clearly state the standards of conduct required.

If staff need to contact a student or parent by phone and do not have access to a work phone, they should discuss this with a senior member of staff and, if there is no alternative, always use 'caller withheld' to ensure the student / parent is not able to identify the staff member's personal contact details.

The live class should be recorded and backed up elsewhere, so that if any issues were to arise, the video can be reviewed.

Retention policy for video recordings

.As these recordings constitute personal data because they contain personal images of identifiable people means that under GDPR, keeping these recordings should be considered as part of the Data Protection Impact Assessment (DPIA).

Briefly this means assessing what data is being captured, why it is held, who can access it, for what reason, and how long will it be kept. Data should only be retained for as long as is necessary to meet the needs of the reason for recording it. 'Data protection: a toolkit for schools' (DfE, 2018) is perhaps the best document to consult here. On page 75, the guidance suggests four ‘tiers’ of retention:

Short term – date of first recording plus 1 month

Medium Term – 1 year

Long Term – 5 years

Very long term – until pupil is 25 years of age or older

It is probably unjustifiable to keep the recordings for the long or very long term, and therefore short term seems sensible but if a lesson relates to something specific that might be referred back to then maybe a little longer.

Other considerations

We also need to remember that not every family is able to afford the required technology and even if they do, there may not be enough to go round the siblings. Families living in poor housing conditions may have no broadband. The gap between the have's and the have-not's will be noticeable with remote learning.

13. Monitoring arrangements

The DSL and/or safeguarding team will log behaviour and safeguarding issues related to online safety on College systems.

This policy will be reviewed annually by the DSL. At every review, the policy will be shared with the board of Trustees.

14. 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 and privacy notices
- Complaints procedure
- COVID-19 Lockdown 21 school closure arrangements for Safeguarding and Child Protection at BRIXHAM COLLEGE
-

Appendix 1: acceptable use agreement (students and parents/carers)

Acceptable use of the College's ICT systems and internet: agreement for students and parents/carers

Name of student:

When using the College's ICT systems and accessing the internet in College, I will not:

- Use them for a non-educational purpose or without a teacher's permission
- Access any inappropriate websites including social networking sites, chat rooms/boards (unless my teacher has expressly allowed this as part of a learning activity)
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share my password with others or log in to the College's network using someone else's details
- Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

I agree that the College will monitor the websites I visit.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the College's ICT systems and internet responsibly.

If I bring a personal mobile phone or other personal electronic device into College I understand that I am only permitted to use them during:

- Social time before and after College
- Break times
- Clubs before or after College, or any other activities organised by the College at the express permission of the teacher

I understand that phones and headphones should be out of sight and silent throughout lesson and transitions unless specifically given permission by staff to use them

Signed (student):	**Date:**
Parent/carer agreement: I agree that my child can use the College's ICT systems and internet when appropriately supervised by a member of College staff. I agree to the conditions set out above for students using the College's ICT systems and internet, and for using personal electronic devices in College, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: acceptable use agreement (staff, Trustees, volunteers and visitors)

Acceptable use of the College's ICT systems and the internet: agreement for staff, Trustees, volunteers and visitors
Name of staff member/Trustee/volunteer/visitor:
When using the College's ICT systems and accessing the internet in College, or outside College on a work device, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature • Use them in any way which could harm the College's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software • Share my password with others or log in to the College's network using someone else's details

I will only use the College's ICT systems and access the internet in College, or outside College on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the College will monitor the websites I visit. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside College, and keep all data securely stored in accordance with this policy and the College's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a student informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the College's ICT systems and internet responsibly, and ensure that students in my care do so too.	
Signed (staff member/Trustee/volunteer/visitor):	**Date:**

Appendix 3: online safety training needs – self-audit for staff

This form or updated versions will be delivered using College Systems/Sharepoint and is attached for demonstration purposes only.

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in College?	
Do you know what you must do if a student approaches you with a concern or issue?	
Are you familiar with the College's acceptable use agreement for staff, volunteers, Trustees and visitors?	
Are you familiar with the College's acceptable use agreement for students and parents?	
Do you regularly change your password for accessing the College's ICT systems?	
Are you familiar with the College's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Risk Assessment for Livestreaming school content

Risk	Mitigation
Inappropriate behaviour or conduct from adults	
Inappropriate behaviour or conduct from children	
Unauthorised recording by pupils, parents, or staff	
Unauthorised sharing of content	
Inappropriate contact with pupils outside lesson time	
Inappropriate contact with pupils in a different account or a different platform	
Inappropriate language in chat function	
Inappropriate dress, conduct, or location	
Unauthorised people invited into the video call	
Unauthorised people crushing into video call	
Unauthorised streaming to another platform	
Unauthorised streaming to the wider public	
Data breach. For example, showing pupils on camera without permission, sharing personal data	
Data breach showing confidential information whilst online	
Unauthorised sharing of inappropriate content via share screen	
Unauthorised lessons that SLT are unaware of	
Accidentally being online early or afterwards without being aware	

Unauthorised chats or video whilst monitoring adult is offline	
Use of livestream platform by unauthorised staff or untrained staff	
What action is to be taken if a disclosure or concern is raised by pupil whilst online?	
How will concerns be raised about any livestream issues by pupils, parents or staff?	
Errors, mistakes, or concerns should be self-reported. How should this be done?	