Online safety policy

Approved by: CEO

Date Approved: 01.12.2022

Version Number: 2

Last Reviewed: 01.09.2025
Next review due by: 01.09.2026

Contents

1. Aims

B2 Mentoring aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and local board members
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole B2 Mentoring 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, fake news, AI, racism, misogyny, self-harm, suicide, anti-Semitism, 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 them 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 scam

2. Legislation and guidance

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

- Teaching online safety in mentoring provisions
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and mentoring provision staff
- Relationships and sex 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.

This policy complies with independent mentoring provision standards.

3. Roles and responsibilities

3.1 The Board of Directors

The board has overall responsibility for monitoring this policy and for its implementation.

The board will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).

All Directors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of B2 Mentoring's ICT systems and the internet (appendix 3)

Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some students with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The Designated Safeguarding Lead

Details of B2 Mentoring's DSL can be found in our child protection and safeguarding policy as well as relevant job descriptions.

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

Ensuring that staff understand this policy and that it is being implemented consistently throughout B2 Mentoring

Managing all online safety issues and incidents in line with B2 Mentoring child protection policy

Ensuring that any online safety incidents are logged on daily reports, incident report and individual safeguarding logs and dealt with appropriately in line with this policy

Ensuring that any incidents of cyber-bullying are logged as above and dealt with appropriately in line with B2 Mentoring behaviour policy

Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)

Liaising with other agencies and/or external services if necessary

Ensuring commissioners are appropriately briefed about incidents.

Providing regular reports on online safety in mentoring provision to the directors, as

required. This list is not intended to be exhaustive.

3.3 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 B2 Mentoring's ICT systems and the internet (appendix 3), and ensuring that students follow B2 Mentoring's terms on acceptable use (appendices 1 and 2)

Working with the DSL to ensure that any online safety incidents are logged on daily reports, incident report and individual safeguarding logs and dealt with appropriately in line with this policy

Ensuring that any incidents of cyber-bullying are logged on daily reports, incident report and individual safeguarding logs and dealt with appropriately in line with B2 Mentoring 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.

3.4 Parents

Parents are expected to:

Notify a member of staff of any concerns or queries regarding this policy

Ensure their child has read, understood and agreed to the terms on acceptable use of B2 Mentoring's ICT systems and internet (appendices 1 and 2)

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

websites: What are the issues? – UK Safer Internet Centre

Hot topics – Childnet International

Parent resource sheet – Childnet International
Healthy relationships – Disrespect Nobody

3.5 Visitors and members of the community

Visitors and members of the community who use B2 Mentoring'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 (Appendix 2).

4. Educating students about online safety

All children will be taught about online safety as part of their provision.

The text below is taken from the National Curriculum computing programmes of study.It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All mentoring provisions have to teach:

Relationships and sex education and health education in secondary mentoring provisions

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

By the **end of secondary mentoring provision**, students will know:

Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online

Not to provide material to others that they would not want shared further and not to share personal material which is sent to them

What to do and where to get support to report material or manage issues online

The impact of viewing harmful content

That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners

That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail

How information and data is generated, collected, shared and used online

How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours

How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

All children who attend B2 Mentoring are defined as vulnerable, all have SEND, some are victims of abuse and have previous history of CSE or CCE. The safe use of social media and the internet is, therefore, regularly covered by mentors who ensure that the curriculum and learning is adapted appropriately..

5. Educating parents about online safety

B2 Mentoring will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

Online safety will also be covered during other communications with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the DSL.

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

6. Cyber-bullying

6.1 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 one person or group by another person or group, where the relationship involves an imbalance of power. (See also B2 Mentoring behaviour regulation policy.)

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.

B2 Mentoring will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Progress leads and mentors will discuss cyber-bullying with their tutor groups, and the issue will be addressed in group sessions and 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, proprietors, 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).
B2 Mentoring 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, B2 Mentoring will follow the processes set out in B2 Mentoring behaviour regulation policy. Where illegal, inappropriate or harmful material has been spread among students, B2 Mentoring 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 Examining electronic devices

Mentoring provision 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 B2 Mentoring 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 mentoring provision discipline), and/or

Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being

abused and that this abuse includes an online element.

Any searching of students will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- B2 Mentoring's COVID-19 risk assessment

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through B2 Mentoring complaints procedure.

7. Acceptable use of the internet during provision

All students, parents, staff, volunteers and proprietors are expected to sign an agreement regarding the acceptable use of B2 Mentoring's ICT systems and the internet (appendices 1 and 2. Visitors will be expected to read and agree to B2 Mentoring's terms on acceptable use if relevant.

Use of B2 Mentoring'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, proprietors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 2.

8. Students using mobile devices in mentoring provision

Students may bring mobile devices into mentoring sessions, they will be allowed to use them at agreed times, within boundaries set by the mentor.
The use of mobile devices should also take into consideration the needs of the individual student and should be managed appropriately.

Any use of mobile devices in mentoring provision by students must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a pupil may result in action in line with B2 Mentoring behaviour policy.

9. Staff using work devices outside mentoring provision

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 are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- 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 – always install the latest updates

Staff members must not use the device in any way which would violate B2 Mentoring's terms of acceptable use, as set out in appendix 3.

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 IT Operations

10. How B2 Mentoring will respond to issues of misuse

Where a pupil misuses B2 Mentoring's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet 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 B2 Mentoring'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 code of conduct or disciplinary policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

B2 Mentoring 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 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).

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:

- o Abusive, harassing, and misogynistic messages
- o Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- o 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 the risks up
- 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 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.

Directors 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.

Training needs identified through individual staff 'self-audits' (Appendix 3), as well as from Mentor Coordinator's and Head of Service's identification of needs.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every year by the Directors. At every review, the policy will be shared with the board. 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.

13. 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

Appendix 1: KS3 and KS4 acceptable use agreement (students and parents/carers)

ACCEPTABLE USE OF B2 Mentoring's ICT SYSTEMS AND INTERNET: AGREEMENT FOR STUDENTS AND PARENTS/CARERS

Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy **When I use B2 Mentoring's ICT systems (like computers) and get onto the internet in mentoring provision I will:** ● Always use B2 Mentoring's ICT systems and the internet responsibly and for educational purposes only ● Only use them when a teacher is present, or with a teacher's permission ● Keep my username and passwords safe and not share these with others ● Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer ● Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others ● Always log off or shut down a computer when I'm finished working on it **I will not:** ● Access any inappropriate websites including: social networking sites, chat rooms and gaming sites 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 ● Log in to B2 Mentoring's network using someone else's details ● Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into mentoring provision:** ● I will only use it during mentoring provision when given permission to do so. ● I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online **I agree that B2 Mentoring will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Signed (parent/carer):	**Date:**

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

ACCEPTABLE USE OF B2 Mentoring's ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, LOCAL BOARD MEMBERS, VOLUNTEERS AND VISITORS

Name of staff member/local board member/volunteer/visitor:	
When using B2 Mentoring's ICT systems and accessing the internet in mentoring provision, or outside mentoring provision on a work device (if applicable), I will not: ● Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) ● Use them in any way which could harm B2 Mentoring'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, or connect unauthorised hardware or devices to B2 Mentoring's network ● Share my password with others or log in to B2 Mentoring's network using someone else's details ● Take photographs of students without checking with teachers first ● Share confidential information about B2 Mentoring, its students or staff, or other members of the community ● Access, modify or share data I'm not authorised to access, modify or share ● Promote private businesses, unless that business is directly related to B2 Mentoring I will only use B2 Mentoring's ICT systems and access the internet in mentoring provision, or outside mentoring provision on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that B2 Mentoring will monitor the websites I visit and my use of B2 Mentoring's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside mentoring provision, and keep all data securely stored in accordance with this policy and B2 Mentoring's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil 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 B2 Mentoring's ICT systems and internet responsibly, and ensure that students in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

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

ONLINE SAFETY TRAINING NEEDS AUDIT

Name of staff member/volunteer:	**Date**:

Question	Yes/No (add comments if necessary)
Are you aware of the ways students can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with B2 Mentoring's acceptable use agreement for staff, volunteers, board members and visitors? Are you familiar with B2 Mentoring's acceptable use agreement for students and parents? Do you regularly change your password for accessing B2 Mentoring's ICT systems?	
Are you familiar with B2 Mentoring's approach to tackling cyber-bullying? Are there any areas of online safety in which you would like training/further training?	

Appendix 4: online safety incident report log

ONLINE SAFETY INCIDENT LOG

Date	Where the incident took place	Description of the incident	Action taken