

STAFF AND LEARNER RELATED POLICY: ONLINE SAFETY POLICY

This policy is annually reviewed to ensure compliance with current regulations

Approved/reviewed by	
Approved by: Deputy Principal Reviewed by: Head of Safeguarding & Wellbeing	
Date of next review	March 2026

This policy and procedure is subject to The Equality Act 2010 which recognises the following Protected Characteristics: Age, Gender Reassignment, Marriage and Civil Partnership, Pregnancy and Maternity, Race, Religion and Belief, Sex, Sexual orientation and Disability

1. Document Control

1.1. Document Details

Title	Online Safety Policy
Author	Matt Smith / Sharon Posey
Version	2.0
Date	March 2025
Status	Published

1.2. Revision History

Version	Date	Author	Comments
1.0	April 2023	Heather Marks / Sharon Posey	Definitive Release
1.1	June 2023	Sharon Posey	Addition to item 3
2.0	March 2025	Sharon Posey	Amendments – Bullet points added within sections 4 and 6

1.3. Distribution

Name	Email	Organisation
All Staff Website All Learners	Uploaded to SharePoint www.boston.ac.uk Microsoft Teams	All Boston College

CONTENTS

- 1. Introduction**
- 2. Online Safety Statement**
- 3. Policy Scope**
- 4. Roles and Responsibilities**
- 5. Filtering and Monitoring**
- 6. Reporting and Responding**
- 7. Online Safety Education and Training**
- 8. Flowchart**

1. Introduction

The growth of different electronic and social media in everyday life and ever developing variety of devices place an additional risk to young people. Social media and networks can be used to contact children and young people with a view to grooming them for inappropriate or abusive relationships, or criminal exploitation. The internet has become a significant tool in the distribution of indecent photographs of children and should be a concern for all staff. It is essential that young people are safeguarded from potentially harmful and inappropriate online material. Learners can engage or be a target of cyberbullying using a wide range of methods to reach their targets.

This Online Safety Policy outlines the commitment of Boston College to safeguard our college community online in accordance with statutory guidance and best practice.

This policy applies to all members of the College community (including staff, governors, learners, visitors, contractors, volunteers) who have access to and are users of college digital systems, both inside and outside of college. It also applies to the use of personal digital technology on the college site (where allowed).

To safeguard the college community and reduce the risks and dangers of online activity, it is essential that all staff and learners are aware of this policy, and that all staff and learners have an understanding and know their responsibilities for online safety.

2. Online Safety Statement

Boston College recognises that online safety is an essential element of safeguarding and duly acknowledges its statutory obligation to ensure that all students and staff are protected from potential online harm. Boston College believes that the internet, social media and associated devices are an integral part of everyday life. Boston College understands that all students should be empowered to build resilience and to develop strategies to recognise and respond to online risks.

3. Policy Scope

This policy supports Boston College in meeting statutory requirements as per the DfE guidance under KCSiE (2022). Effective, timely and robust online safety is critical to protecting young people in education and it is a significant part of the safeguarding agenda.

Defining online abuse: “Online abuse is any type of abuse that happens on the web, whether through social networks, playing online games or using mobile phones” (NSPCC, 2019).

While technology can facilitate a world of learning and development in addition to creating opportunities, the stark reality is that it can also lead to potential and actual harm and abuse. It can elicit and support a wide range of illegal abusive behaviours.

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

- Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- Contact: being subjected to harmful online interaction with other users; for example: 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: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g., consensual or non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.
- Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Hidden harms – types of online abuse may include, but are not limited to:

- Cyberbullying
- Harassment/Stalking
- Threatening behaviour
- Emotional abuse
- Grooming
- Sexting
- Sexual abuse/exploitation/harassment
- Criminal exploitation
- Radicalisation/Extremism
- Blackmail/Extortion e.g., to send nude/inappropriate pictures, to extort money
- Hate Crime
- Sharing of inappropriate/illegal material

Other factors to consider include:

- Recognising that learners behave differently online as they feel protected with anonymity and invisibility. This can cause them to take risks where they perhaps wouldn't otherwise outside of the online platforms.
- Understanding that learners can often pass off unacceptable or harmful online behaviours as so-called social norms or just banter. For example, language that can be used, and in some cases is often expected, as part of online gaming and the normalisation of misogynistic, homophobic and racist language that would never be tolerated offline.

4. Roles and Responsibilities

To ensure the online safeguarding of members of our community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become

apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the College.

Boston College has used learner focus groups to inform this policy about the day to day risks they face online.

The Principal and CEO:

Has a duty of care for ensuring the safety (including online safety) of the college community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety may be delegated to the Designated Safeguarding Lead.

The Head of IT and Designated Safeguarding Lead:

Have a responsibility to review and ensure that this policy is meeting statutory guidance and best practice.

The DSL and safeguarding team are responsible to:

- ensure young people are being appropriately taught about and know how to use the internet responsibly by providing resources as appropriate for tutorial sessions.
- take responsibility for all safeguarding matters, including online safety.
- ensure effective record keeping and the reporting and monitoring of all online safety concerns.
- promote online safety and the adoption of a whole college approach.
- maintain own training and learning needs, ensuring they are up to date with all matters relating to online safety.
- provide online safety information to parents (website/newsletters).

Head of IT is responsible to ensure that:

- they are aware of and follow the college Online Safety Policy and Information Security Policy to carry out their work effectively in line with statutory guidance.
- the college technical infrastructure is secure and is not open to misuse or malicious attack.
- there is clear, safe, and managed control of user access to networks and devices
- they keep up to date with online safety technical information to effectively carry out their online safety role and to inform and update others as relevant
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be investigated and actioned
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
- monitoring software/systems are implemented and regularly updated

Curriculums have a responsibility to deliver mandatory online safety sessions within tutorial sessions and encourage online safety throughout delivery.

All staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding.
- they immediately report any suspected misuse or problem to the college safeguarding team for investigation/action, in line with the College safeguarding procedures
- all digital communications with learners and parents/carers should be on a professional level and only carried out using official college systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other activities (where allowed)
- they adhere to the college's Professional Code of Conduct policy.
- their own online activity does not impede on professional reputation or bring the College into disrepute.

Learners have a responsibility to ensure that they:

- are using the college's digital technology system in accordance with the Computer Use and Digital Code of Conduct and Online Safety Policy (this should include personal devices – where allowed)
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- should know what to do if they or someone they know feels vulnerable when using online technology.
- should understand the importance of adopting good online safety practice when using digital technologies out of college and realise that the Online Safety Policy covers their actions out of college, particularly if there is bullying or harassment or safeguarding concerns.

Parents and Carers should ensure that they:

- Read and adhere to all relevant policies.
- Are responsible when taking photos/using technology at college events
- Know who the college Senior DSL is.
- Know how to report online issues.
- Support online safety approaches and education provision.

- Are a role model for safe and appropriate behaviour.
- Identify changes in young people's behaviour that could indicate they are at risk of online harm or abuse.

5. Filtering and Monitoring

Filters and monitoring systems are in place on internal IT systems to provide learners and staff with a safe environment in which to learn and to limit learners' exposure to risk of harm and/or abuse to inappropriate material.

These systems are monitored by the IT team and safeguarding team using daily reports and e-mails from the software providers to alert of any unsafe or harmful content.

6. Reporting and Responding

The college will take all reasonable precautions to ensure online safety for all users but recognises that incidents may occur inside and outside of the college which may need intervention. The college will ensure:

- there are clear reporting routes which are understood and followed by all members of the college community which are consistent with the safeguarding procedures.
- all members of the college community will be made aware of the need to report online safety issues/incidents.
- Staff support learners to report concerns directly to relevant social media platforms.
- reports will be dealt with as soon as is practically possible once they are received.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm, the incident must be escalated through college safeguarding procedures.
- any concern about staff misuse will be reported to the Designated Safeguarding Lead, unless the concern involves the Principal and CEO, in which case the complaint is referred to the Chair of Governors and the local authority.
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- To access support as deemed appropriate from the police, the National Crime Agency's Click CEOP reporting service for children and 3rd sector organisations, such as Childline and the Internet Watch Foundation.
- incidents should be logged on VITAL for learners or on HR records for staff.
- Serious safeguarding issues will be logged within confidential safeguarding files

If learners have any concerns regarding online safety, they can: -

- Report to their tutor or other trusted adult in the college verbally, on teams and by e-mail.
- Report to Learner Services and/or safeguarding team direct verbally, on teams and by e-mail

If staff observe or are notified of any concerns online, they must: -

- Record details of concern and if relevant and appropriate collate evidence
- Report to Learner Services or Safeguarding Team
- Learner Service and/or Safeguarding will ascertain whether this is to be dealt with under the Safeguarding Policy and/or the Bullying and Harassment Policy
- If an illegal act has been disclosed/observed, then the Police must be informed.

The college will make the flowchart (appendix 1) available to staff to support the decision-making process for dealing with online safety incidents.

7. Online Safety Education and Training

To ensure staff can respond appropriately the college will:

- Ensure provision of policies and practices as part of induction and ongoing training provision.
- Provide up to date online safety training at least annually or more, in line with legislative and statutory changes and/or online safety incidents arising.
- Inform staff and learners of monitoring and filtering processes.
- Make staff aware that their online conduct outside of work can impact upon their professional role and responsibilities.
- Advise of appropriate resources.
- The Head of IT and DSL and safeguarding team will complete the annual online safety certificate provided via National Online Service to keep up to date with changes/emerging trends

To ensure learners are safe and responsible online, the college will:

- Educate learners regarding safe and responsible use and access of the internet.
- Follow Education for a Connected World – 2020 Edition to equip learners with relevant information about specific aspects of online safety.
- Include online safety as mandatory in Make a Difference tutorial sessions.
- Reinforce online safety messages during curriculum delivery.
- Include annual mandatory online safety training for staff via National Online Safety training platform.

Boston College uses National Online Safety to provide information, guidance and training to staff, governors, learners and parents and carers. This enables the college to track and report on training undertaken by college staff.

This policy is to be used alongside the following College Policies:

Safeguarding Learners

[Safeguarding Students Policy.pdf](#)

Social Media

[Boston College Social Media Policy.pdf](#)

Disciplinary Procedure and Code of Professional Conduct

[Disciplinary Procedures and Code of Conduct.pdf](#)

Whistleblowing

[Whistleblowing Policy.pdf](#)

Computer Services: Unit Code of Practice

[Computer Services Unit Code of Practice.pdf](#)

Appendix 1: Flowchart – Reporting a concern.

