1. Document Control

1.1. Document Details

Title	Online Safety Policy
Author	

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**

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
  f 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

Curriculums have a responsibility to deliver mandatory online safety sessions within tutorial sessions and

- 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

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

Document Centre - Safeguarding Learners.pdf - All Documents (sharepoint.com)

Social Media

Document Centre - Social Media.pdf - All Documents (sharepoint.com)

Disciplinary Procedure and Code of Professional Conduct

Document Centre - Disciplinary Procedures and Code of Conduct.pdf - All Documents (sharepoint.com)

Whistleblowing

Document Centre - Whistleblowing Policy.pdf - All Documents (sharepoint.com)

Computer Use and Digital Code of Conduct

Computer Services Unit Code of Practice.doc (sharepoint.com)

Appendix 1: Flowchart Reporting a concern.