E-Safety Policy

Date created: November 2019

Review date:	Reviewed by:	Next review date:
November 2021	Selina Hayes	November 2023
August 2023	Selina Hayes	August 2025

Contents

1.0. Introduction

Blackpool FC Community Trust (all facilities) recognises the benefits and opportunities which new technologies offer to teaching and learning. Our approach is to ensure that safeguards are in place to support all staff and learners to identify and manage risks.

We believe this can be achieved through a combination of security measures, training and guidance alongside implementation of other relevant policies.

This e-safety policy should be read in conjunction with other relevant policies and procedures including safeguarding, IT acceptable use, Anti-bullying, Whistleblowing and Disciplinary policies.

2.0. Definition of E-Safety

The term e-safety is defined for the purposes of this document as the process of limiting the risks to children, young people and Adults at Risk when using Internet, Digital and Mobile Technologies (IDMTs) through a combined approach to policies and procedures, infrastructures and education, including training, underpinned by standards and inspection. E-safety risks can be summarised under the following three headings.

2.1. Content

- Exposure to age-inappropriate material
- Exposure to inaccurate or misleading information (fake news)
- Exposure to socially unacceptable material, such as that inciting violence, hate, extremism or intolerance
- Exposure to illegal material, such as child abuse images
- Illegal downloading of copyrighted materials e.g. music and films

2.2. Contact

- Grooming using communication technologies, potentially leading to sexual assault or child prostitution
- Radicalisation, the process by which a person comes to support terrorism and extremist ideologies
- Bullying via websites, mobile phones or other forms of communication device

2.3. Commerce

- Exposure of minors to inappropriate commercial advertising
- Exposure to online gambling services
- Commercial and financial scams

3.0. Scope

This policy applies to everyone who has access to the Blackpool FC Community Trust IT systems (inclusive of BFC School and BFC Sports College), both on premises and remote access. Any user must adhere to e-Safety rules and the IT acceptable use policies.

The e-Safety Policy applies to all use of the internet, and electronic communication devices such as email, mobile phones, games consoles, social networking sites, and any other systems that use the internet for connection and providing of information.

4.0.Aims

The aims are to:

4.1. To ensure safeguards on BFCCT IT-based systems are strong and reliable

4.2. To ensure user behaviour is safe and appropriate

4.3. To assure that the storage and use of images and personal information on BFCCT systems is secure and meets all legal requirements

4.4. To educate staff and learners in e-Safety

4.5. To ensure any incidents which threaten e-safety are managed appropriately

5.0.Outcome

5.1. Security, Filtering and

BFCCT networks are safe and secure, with appropriate and up to date security measures and software in place.

BFCCT networks will filter inappropriate searches, blocking access to sites that are deemed unsafe e.g. pornography, gambling

As part of their duty of care BFCCT staff will to the best of their ability monitor what participants are accessing through mobile networks. Anyone under the age of 18 sending or receiving inappropriate material must be reported on MyConcern.

Any breach in security or failed filtering will be reported to IT and the Designated Safeguarding Lead using the Filtering Breach Report Form.

The reporting procedure for filtering and monitoring can be found in appendix 1.

Further information on filtering and monitoring can be found in Keeping Children Safe in Education 2023.

5.2. Risk assessment

When making use of new technologies and online platforms, assessment of the potential risks of utilising that technology is undertaken.

5.3. Behaviour

- It is unacceptable to download or transmit any material which might reasonably be considered obscene, abusive, sexist, racist, defamatory, related to violent extremism or terrorism or which is intended to annoy, harass, or intimidate another person. This also applies to the use of social media accessed through BFCCT systems

- All users of technology adhere to the standards of behaviour set out in the IT Acceptable Use policy
- All users of IT adhere to BFCCT guidelines when using email, mobile phones, social media platforms, game consoles, chat rooms, video conferencing and webcams
- Any abuse of IT systems and any issues of bullying or harassment (cyber bullying) are dealt with seriously, in line with staff and student disciplinary procedures
- Any conduct considered illegal is reported to the police
- Staff must take responsibility for moderating any content posted online
- Staff should be aware of cyber bullying, grooming, grooming law and child protection issues and forward any concerns to the Designated Safeguarding Officer
- Staff should keep personal and professional lives separate online
- Staff should not have students as 'friends' on social media sites that share personal information
- Staff should be wary of divulging personal details online and are advised to investigate privacy settings on sites to control what information is publicly accessible.
- Staff should recognise that they are legally liable for anything they post online.
- Staff are always expected to adhere to the college's equality and diversity policy and not post derogatory, offensive or prejudiced comments online.
- Staff should not bully or abuse colleagues/students online.
- Staff entering into a debate with a student online should ensure that their comments reflect a professional approach.
- Staff should not post any comments online that may bring the college into disrepute or that may damage the college's reputation.
- Staff wishing to debate and comment on professional issues using personal sites, should be aware that this may be seen as a reflection of college views, even with a disclaimer, and should consider their postings carefully.
- Staff should not use their college e-mail address to join sites for personal reasons or make their college e-mail address their primary contact method.
- Staff should be aware that any reports of them undertaking inappropriate online activity that links them to the College will be investigated and may result in disciplinary action.

5.4. Use of images and video

- The use of images or photographs is encouraged in teaching and learning. Providing there is no breach of copyright or other rights of another person
- Staff and learners are informed of the risks involved in downloading, posting and sharing images, and particularly the risks in posting personal images onto social networking sites
- College staff provide information to learners on the appropriate use of images, and on how to keep their personal information safe
- Advice and approval from a senior manager are sought if there is any doubt about the publication of any materials.

5.5. Personal

- Processing of personal information is done in compliance with the Data Protection Act 2018
- Personal information is kept safe and secure in line with the BFCCT Data Protection Policy. This includes the sharing and storage of data
- All data stored online or electronically is password protected
- Any mobile devices that store personal information are encrypted and password protected in line with the BFCCT Data Protection and Bring your own device policies)
- Personal data that is no longer required is destroyed or deleted appropriately.

5.6. Education and Training

- Staff and learners are supported through training and education to develop the skills to identify e-safety risks independently
- Learner inductions and the tutorial programme contains lessons on e-safety
- Learners are guided in e-safety across the curriculum and opportunities are taken to reinforce e-safety messages
- Learners know what to do and who to talk to where they have concerns about inappropriate content, either where that material is directed to them, or discovered as part of a random search.
- In class, learners are encouraged to question the validity and reliability of materials researched, viewed or downloaded. They are encouraged to respect the copyright of other parties and to cite references appropriately
- All users are to read, sign and agree the acceptable use policy.

6.0. Incidents and response

- A clear and effective incident reporting procedure is maintained and communicated to learners and staff.

- Reports of e-safety incidents are acted upon immediately to prevent, as far as reasonably possible, any harm or further harm occurring.

- Action following the report of an incident might include disciplinary action, sanctions, reports to external agencies (e.g. the police), review of internal procedures and safeguards, tutor support for affected learners, etc.

7.0. Responsibilities

The Designated Safeguarding Officer is responsible for:

- Maintaining this policy, and to ensure that best practice is communicated to all staff, learners and participants.
- Ensuring that reportable e-safety matters are referred to the relevant organisations

The following staff are responsible for implementing it:

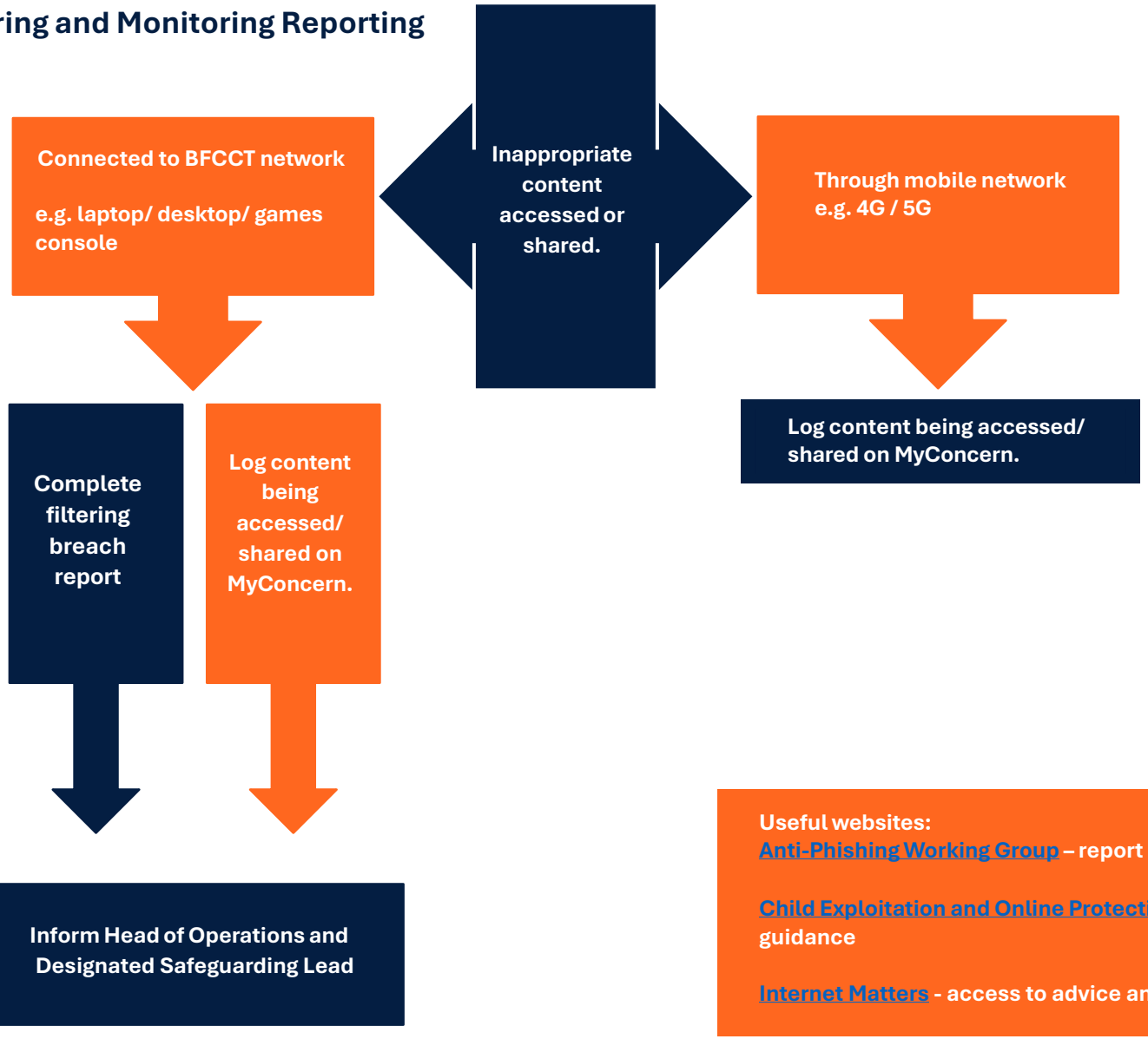
- All managers for implementing good e-safety practice and safeguards consistent with this policy in their area of responsibility
- All delivery staff employed by BFCCT in ensuring that they make participants aware of how to be safe online and the consequences attached to incidents such as cyberbullying
- IT service provider for providing technical expertise when issues are being investigated

8.0.Access and review of the policy

This policy will be accessible on the shared drive within Policies – Safeguarding folder.

This policy will be reviewed every two years or following reportable e-safety concerns.

Filtering and Monitoring Reporting



Remember the four C's:

Content: is the content illegal, inappropriate, harmful e.g., fake news, racism, extremism

Contact: are users being subjected to harmful online interaction e.g., adults posing as children, peer to peer pressure

Conduct: are users sending and receiving explicit images (consensual or non-consensual), online bullying

Commerce: online gambling, phishing scams, inappropriate advertising

Useful websites:
Anti-Phishing Working Group – report phishing scams

Child Exploitation and Online Protection (CEOP) – access to advice and guidance

Internet Matters - access to advice and guidance