



E-Safety Policy

Introduction

E-Safety is in place for not only staying safe on the internet, but also other electronic forms of communication, such as wireless technology and mobile phones. The purpose of e-safety is to safeguard all activity on electronic devices and the internet, as well as raising awareness of how to stay safe.

BloR promote the use of using the internet and other forms of technology to work and learn, however, doing so in a suitable manner. As technology and the internet are easily accessible, it also unfortunately means that every user could face potential risks and consequences. BloR Business School practice safe working through providing guidance, ensuring security measures are in place, and making everyone aware of our policies.

Any incidents regarding e-safety are to be reported to the Safeguarding Team

Designated Safeguarding and PREVENT Lead

Chetna Vaghjiani

Email: chetna.vaghjiani@ior.org • Email: safeguarding@ior.org

Telephone: 0161 226 8436 or 07387 815 359

Deputy Designated Safeguarding and PREVENT Lead

Azmat Mohammed

Email: azmat.mohammed@ior.org

Telephone: 07866529010


All Apprentices are Safeguarded by BloR Business School and use of digital technology is in accordance with the companies Safeguarding and Prevent agenda and policies.

This policy is intended to ensure –

- That all users will be responsible and stay safe while using the internet and other communications technologies for professional, personal and recreational use.
- BloR Business School systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Individuals are protected from potential risk in their use of technology in their everyday work.

Use of Internet

The internet is essential for most workplaces and is used constantly in day-to-day life. There are many advantages of the internet and its uses, however, there are also plenty of risks that result in using it.



When visiting websites, it is a possibility that you may come across malicious and/or inappropriate websites with the following risks;

- **Viruses & Spyware (Malware)**
- **Phishing (obtaining your personal/financial details to possibly steal identities)**
- **Fraud**
- **Copyright violation (illegally copying/downloading protected images, software, documents etc.)**
- **Being exposed to inappropriate content**

At BloR Business School we ensure every PC has the highest security measures to prevent any risks occurring, however, you must be aware of the known risks.

E-Safety Policy

General tips;

- **Never enter any personal/financial information into PC's/laptops/mobile phones**
- **Always ensure the websites you are visiting are secure (the website address should begin with 'https://' – the 's' stands for 'secure')**
- **Use a well-known, safe browser e.g. Internet Explorer, Google Chrome, Safari etc.**
- **Ensure you have effective anti-virus, anti-spyware and firewall software installed**
- **Report any inappropriate material to your assessor who will then forward it over to the IT department**

Use of Email

In addition to the internet, it is extremely important to use email safely and be cautious of sending and receiving mail. There are a few points to consider when using email;

- **Never click on links or open attachments from unknown senders or suspected fraudulent senders**
- **Do not respond to, or forward on, emails from unknown senders or suspected hoax senders**
- **Report any scam emails and spam to the IT team who will then take the appropriate action**

Your Responsibility


Your responsibility is to report any incidents regarding e-safety either to the IT Department or directly to the Safeguarding team. You are also responsible for ensuring you use all systems and devices in accordance to our policies and procedures.

Data Protection

BloR Business School take data protection very seriously and ensure that any sensitive information about an individual is secure. We also make sure that any personal or sensitive information about an individual is not shared with any third party without the consent of that individual. Measures to take to comply with data protection include password protecting all resources,

Plagiarism

Plagiarism is not just when you directly copy words from another's work. Plagiarism also occurs



when you re-word someone else's ideas in your own work and you do not give credit to the original source. Plagiarism can have a very negative impact. Further action may be taken if you are found to have plagiarised repeatedly, this could lead to disqualification and dismissal of an apprenticeship or the workplace. On a more positive note, referencing is important for reasons other than avoiding plagiarism. When you reference correctly you are demonstrating that you have read and researched your topic in detail. This lends credibility to your own work as well as allows your work to be checked to validate of your arguments for themselves. Please do not take advantage of the use of technology to commit plagiarism.

BloR Business School E-Safety Policy Statements

- I will not purposely access sites which contain items that are illegal, insulting, pornographic or in any way offensive.
- I will observe the laws and policies regarding copyright and plagiarism.
- I will not download files to any BloR Business School's computer/laptop.
- I will observe the requirements of Data Protection and take appropriate steps to protect all personal data.
- I will report any unsafe or inappropriate material or information found to the IT department or the Safeguarding Lead.
- I agree that I shall not write or send malicious or offensive e-mails and accept that, if I do, I will be reported to the Safeguarding Lead and appropriate actions will be taken.
- I understand that if I am involved in any form of cyber bullying, that this will be dealt with in line with BloR Business School's Anti-Bullying Policy.
- I will never give my log in details to anyone else or attempt to access the network using a log in that is not my own.
- I will never slander staff, students or BloR Business School on a social networking site, e.g. Facebook, Twitter, Snapchat etc.
- I understand that the BloR Business School may monitor my use of the systems, devices and digital communications.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- I will report directly any activity that refers to Safeguarding or Prevent directly to the DSO or DDSO
- I will not use the BloR Business School systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting – unless authorised.
- If using any personal devices such as (laptops / tablets / mobile phones) in the business, these must only be connected to the guest WIFI (where provided) these devices **MUST NOT** be connected to the staff network.
- I will not use personal email addresses on BloR Business School ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any BloR Business School device, nor will I try to alter computer settings.
- I understand that BloR Business School also has the right to act against me if I am involved in incidents of inappropriate behaviour, that are covered in this policy, when I am out of BloR Business School premises and where they involve my involvement of the BloR Business School community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Policy, I will be subject to disciplinary action. This may include loss of access to the BloR Business School network / internet, suspensions, disciplinary, contact with parents and employers and in the event of illegal activities involvement of the police.

E-Safety Policy

An example of categories that are blocked –

Adult/Sexually Explicit Alcohol & Tobacco Criminal Activity Hacking
Illegal Drugs
Intimate Apparel & Swimwear Intolerance & Hate
Sex Education Tasteless & Offensive Violence
Weapons
Personals & Dating Gambling
Games

This list is in no way exhaustive.

Version 3.0

Date Approved by Governance Board 18/3/2019

Date of Next Review 18/3/2020



BloR
Business School

Suite 7, First Floor,
Parkway 2, Princess Road,
Manchester M14 7LU
Company Reg: 07575583
VAT No: 117 9788 66
Phone: +44 (0)871 288 2108
Email: support@ior.org