

e-Safety Policy

Introduction

Babington recognises the advantages that new and emerging technologies provide for both teaching, learning and assessment; however, with the global nature of online, its accessibility, and the variety of technologies at our disposal, we are more aware of the possible risks and challenges associated with such freedom of access.

Virus protection, internet filtering, firewalls, DNA alerts, and other IT security safeguards are all part of e-safety. E-Safety also entails making sure that technology is utilised in a way that is both safe and respectful of others. Due to this E-Safety has a significant overlap with other policies and procedures and should be read in conjunction with the Acceptable Use of Information and Communications Technologies (ICT) Policy and the Social Media Policy that are located on BORIS/policies/ Information Security. It is also to be read in conjunction with the Safeguarding and Prevent Policy Handbook which includes the Anti-Bullying Policy

This e-Safety Policy outlines the learner and safeguarding context for the use of the internet and social media and specifies the roles and responsibilities of all those who have access to Babington ICT, with specific reference to learners, staff, visitors and Designated Safeguarding Leads.

What is e-Safety?

According to the Chartered Institute of Public Relations (CIPR), social media are: *“Internet and mobile based channels and tools that allow users to interact with each other and share opinions and content. It involves the building of communities or networks and encouraging participation and engagement.”* This is the recognised definition for the purpose of this document.

The term e-safety is defined for the purposes of this document as the process of limiting the risks to staff, learners and authorised contractors when using Internet, Digital and Mobile Technologies (IDMTs) through a combined approach to policies and procedures, infrastructures and education, including training.

Scope

This e-Safety Policy applies to all staff, learners, visitors and contractors who have access to, or are users of, Babington ICT systems and resources, both in and out of learning venues, in the workplace or through distance learning, e.g. internet, electronic communications, Virtual Learning Environment (VLE) or mobile devices.

Learner Context

To prepare learners for the needs of today and their future working lives where the curriculum and their personal goals require them to learn how to locate, retrieve and exchange information using a variety of technologies, computer skills are vital to access employment and life-long learning as ICT is now seen as an essential skill for life. However, technologies present risks to vulnerable groups as well as benefits.

Internet use for work, home, social and leisure activities is expanding across all sectors of society. This brings our staff and learners into contact with a wide variety of influences some of which may be unsuitable. These new technologies are enhancing communication and the sharing of information, which inevitably challenge the definitions and boundaries of the learning environment.

Current and emerging technologies in the learning environment and more importantly, in many cases used outside the learning environment by learners include:

- Internet websites
- Virtual Learning Environments (VLE)
- Instant messaging
- Social networking sites
- E-mails
- Blogs
- Podcasting
- Video broadcasting sites
- Chat rooms
- Gaming and gambling sites
- Music download sites
- Mobile phones with camera and video functionality
- Digital cameras
- Smart phones, iPads and Tablets with e-mail and web applications.

All of these technologies have potential to help raise standards of teaching learning and assessment but may equally present challenges to both learners and trainers in terms of keeping themselves safe.

Benefits and Risks

Effective use of social media can bring significant and measurable benefits to Babington. These include opportunities to promote the organisation's success stories, develop national and potentially international reach, improve learner engagement and attract high quality staff, learners and new business. Social media channels can spread the organisation's messages quickly and to a large range of audiences at little or no cost and, unlike other traditional media channels, they provide instant feedback from those audiences.

Babington provides internet access to all staff, learners and authorised contractors, and encourages the use of technologies to enhance skills, promote achievement, enable lifelong learning and develop the business.

Along with these benefits come the risks inherent in managing something that is as dynamic and unlimited in scale. These include the risk of reputational damage arising from misuse by staff, learners or third parties, threats to the security of sensitive or confidential information, exposure to malware and a negative impact on productivity. e-Safety must be responsive to new technologies and new threats and opportunities that may arise.

When a learner, staff member, visitors or contractor initiates, or is the victim of, an activity that uses Information and Communications Technologies linked to the personal safety, mental well-being, or financial well-being of another individual, it is deemed an e-Safety incident.

e-Safety risks can be summarised under the following three headings:

Content

- Exposure to inaccurate or misleading information
- Exposure to socially unacceptable and inappropriate material, such as that inciting violence, hate or intolerance, sites promoting radicalisation or pornography
- Exposure to illegal material, such as images of child abuse
- Illegal downloading of copyrighted materials e.g., music and films

Contact

- Grooming using communication technologies, potentially leading to sexual assault, sexual exploitation and radicalisation
- The use of assumed identities on gaming platforms
- Identity theft or invasion of privacy
- Cyber-bullying via websites, social media, mobile phones or other forms of communication device or technologies
- Spyware, e.g. use of Remote Access Trojans/Tools to access private information or spy on their victim

Commerce

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

The requirement to use the Internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work for and with the company are bound. This e-Safety policy should help to ensure safe and appropriate use for all staff, learners, visitors and authorised contractors and help them manage and detect risks on their own, as well as seek appropriate and timely advice and guidance.

Roles and Responsibilities

The key responsibilities of the Designated Safeguarding Lead/ Safe and Sound Team are:

- Acting as a named point of contact for all online safeguarding and e-safety incidents and liaising with other members of staff and other agencies as appropriate.
- Keeping up to date with current research, legislation and trends regarding online safety.
- Coordinating participation in local and national events to promote positive online behaviour.
- Maintaining a record of online safety concerns/incidents and actions taken as part of the safeguarding recording structures and mechanisms.
- To investigate and report any DNA alerts / Keywords that could identify a person may be at risk of or experiencing online abuse, harm or intending to cause abuse or harm.
- Reporting to the Board of Directors and other agencies as appropriate, on online safety concerns and local data/figures.
- Liaising with the local authority and other local and national bodies, as appropriate.
- Working with senior management to review and update the online safety policies, Acceptable Use Policies (AUPs) and other related policies on a regular basis (at least annually) with stakeholder input.
- Ensuring that online safety is integrated with other appropriate company policies and procedures.
- Leading an online safety team/group with input from all stakeholder groups.
- Meet regularly with the board member with a lead responsibility for online safety.

The key responsibilities for all members of staff and authorised contractors are:

- Contributing to the development of online safety policies.
- Reading the Acceptable Use of ICT Policy and the Social Media Policy and adhering to them.
- Taking responsibility for the security of company information systems and data.
- Having an awareness of a range of different online safety issues and how they may relate to the learners in their care and their colleagues.
- Modelling good practice when using new and emerging technologies.
- Embedding online safety education in learner delivery wherever possible.
- Identifying individuals of concern and taking appropriate action by following safeguarding policies and procedures.
- Report any breaches or concerns to the Information Security Team and ensure the appropriate action is taken as advised.
- Knowing when and how to escalate online safety issues, internally.
- Being able to signpost to appropriate support available for online safety issues, internally.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site.
- Demonstrating an emphasis on positive learning opportunities.
- Taking personal responsibility for professional development in this area.

In addition to the above, the key responsibilities for staff managing the technical environment are:

- Providing a safe and secure technical infrastructure which support safe online practices whilst ensuring that learning opportunities are still maximised.
- Taking responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team.
- To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on company-owned devices.
- Ensuring that the filtering policy is applied and updated on a regular basis.
- Ensuring that the use of the network is regularly monitored and reporting any deliberate or accidental misuse to the Information Security Manager (ISM).
- Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.
- Report any breaches and liaise with the Information Security Team as appropriate on technical infrastructure issues.
- Providing technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Ensuring that the ICT infrastructure/system is secure and not open to misuse or malicious attack.
- Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.
- Ensure that appropriately strong passwords are applied and enforced for all users of company ICT equipment.

The key responsibilities of Learners:

- Respecting the feelings and rights of others both on and offline.
- Seeking help from their trainer if things go wrong and supporting others that may be experiencing online safety issues and report to the Safeguarding team
- Taking responsibility for keeping themselves and others safe online.

- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Assessing the personal risks of using any technology and behaving safely and responsibly to limit those risks.

Legislation

The legal framework for the role of Babington and the governing body is as follows:

Computer Misuse Act 1990 : UK law that protects personal data held by organisations from unauthorised access to computer systems and modification of files without consent.

Data Protection Act 1998 : Makes provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information.

Malicious Communications Act 1988 : A British Act of Parliament that makes it illegal in England and Wales to "send or deliver letters or other articles for the purpose of causing distress or anxiety". It also applies to electronic communications.

Counter-Terrorism and Security Act 2015 : A duty on specified authorities to include the further and higher education sectors to have due regard to the need to prevent people from being drawn into terrorism. This is also known as the Prevent duty.

The Education Act 2002 - Section 157 & 175 : Requires local authorities and governing bodies of further education institutions to make arrangements to ensure that their functions are carried out with a view to safeguarding and promoting the welfare of children, young people, and adults at risk. In addition, they should have regard to any guidance issued by the Secretary of State in considering what arrangements they may need to make

Working together to Safeguard Children 2018 : This guidance sets out what organisations and agencies who work with children must and should do to safeguard and promote the welfare of all children and young people under the age of 18, including identifying and responding to their needs.

The Mental Capacity Act 2005 : Provides a means for persons who may require assistance in making decisions to receive that assistance from someone who can be trusted to behave in their best interests. The Act applies to those age 18 and over and applies to those who are 16 and 17 years of age, except making Power of Attorney or Making a Will. In very limited circumstances, the Act would apply to those under 16 whereby it would be determined by a court.

Breach of Legislation or Policy

Serious offences may lead to job or training dismissal and possibly prosecution, the penalties of which may include a custodial sentence.

Any suspected breach of this policy may result in disciplinary action and must be reported as an Information Security Incident (as per the Information Security Incident Reporting Procedure) to the Information Security Team who will conduct/arrange appropriate enquiries.

Additional Guidance

In support of this policy, the following online sites provide further information in relation to e-Safety and the use of social media and the Internet:

Staying Safe Online – People First:

<https://www.peoplefirstinfo.org.uk/staying-safe/staying-safe-on-line.aspx>

Get Safe Online: 'The Rough Guide to Online Safety': <https://www.getsafeonline.org/get-safe-online-around-the-world/>

Thinkuknow:

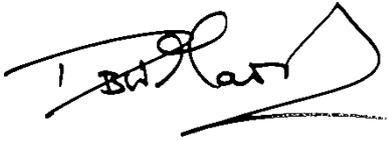
<https://www.thinkuknow.co.uk/>

Online Safety – NSPCC:

<https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/>

BullyingUK:

<http://www.bullying.co.uk/cyberbullying/how-to-stay-safe-online/>

CEO Name :	David Marsh
CEO Signature:	
Date:	02/11/2021

The Safe & Sound Manager and Information Security Manager are the joint owners of this document and have approved its publication. The document owners are responsible for ensuring that this procedure is reviewed annually.

This document is issued on a version-controlled basis and is available to all colleagues on the corporate intranet

Document Management:

Owner: Safe & Sound Manager and Information Security Manager
 Effective Date: 02/11/2021
 Review Date: 02/11/2022
 Document reference: DOC 3206 e-Safety Policy

Change History Record

Version control	Substantive change narrative	Author of substantive change	Date of substantive change
0.1	Draft Version	ISM	
0.2	Add summary to beginning of document	ISM	
1.0	Final ratification	CEO	01/06/2018
2.0	Amended by ISM following implementation of ISMS and Policy ownership designated to Group Safe & Sound Manager	Safe & Sound Manager	28/06/2018
3.0	Reviewed document and amendments made to wording	Safe and Sound Manager	06/02/2020
4.0	Review date extended to May	Safe & Sound Manager	02/03/2021
5.0	Introduction expanded on, wordings to the document and legislation added	Safe and Sound Manager	02/11/2021