e-Safety Policy for Staff and Learners

Basingstoke ITEC Limited recognises the benefits and opportunities which new technologies offer to teaching and learning. We provide internet access to all learners and staff and encourage the use of technologies to enhance skills and promote achievement. However, the accessibility and global nature of the internet and different technologies mean that we are also aware of potential risks and challenges associated with such use. Our approach is to implement appropriate safeguards whilst supporting staff and learners to identify and manage risks independently and with confidence. The purpose of this policy is to convey the approach that Basingstoke ITEC Limited will take to identify and manage risks, safeguard and support staff and leaners, and promote the safe use of technology.

Scope

The policy applies to all learners, staff, Board Members and any other users of the company's premises or systems who have access to the ICT systems, both within the building and remotely.

The policy applies to all use of the intranet and electronic communication tools such as, but not limited to, email, mobile phones, tablets, smart phone applications and social networking sites.

Definitions

e-Safety encompasses all internet technologies and electronic communication tools such as laptops, iPads, mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate users about the benefits and risks of using technologies and provides safeguards and awareness to enable them to control their online experience.

Information Communications Technology (ICT) consists of all technical means used to handle digital information and aid communications, including computer and network hardware, software and data and information management.

Social Networking sites are App and web-based services that allow individuals to construct a public or semi-public profile within a bounded system to interact with other users. Social networking sites usually have a new user input a list of people with whom they share a connection and then allow the people on the list to confirm or deny the connection.

Personal Data is data which relates to a living individual and which could allow the individual to be identified from the data.

Key Principles

ICT Security

Basingstoke ITEC Limited takes steps to ensure that the networks are safe and secure to protect both users and the company. Security software is kept up to date and a range of security measures are in place within the company to prevent accidental or malicious access of systems and information. These measures include; Firewalls, Anti-virus software, Blocking of inappropriate sites, internet usage and Password management.

Risk Assessment

For Basingstoke ITEC Limited to make available any technologies and/or online platforms, it is necessary to access any potential risk whilst considering the planning of such technologies. The assessment of risk allows both level and nature of risk to both users of the ICT systems and the company to be determined and for corresponding risk management to be implemented. Risk is assessed and considered before any new or emerging technology is made available to staff or learners on the company's systems.

Acceptable Use

Basingstoke ITEC Limited requires all users of its ICT systems and networks to adhere to the standard of behaviour as set out in the ICT Acceptable Use Policy and for staff to work within the guidance detailed within the Safeguarding Policy.

Unacceptable conduct will be treated seriously and in line with learner and staff disciplinary codes and procedures, or other company protocol as appropriate.

Where conduct is found to be unacceptable, Basingstoke ITEC Limited will normally deal with the matter internally, however where conduct is considered to be illegal, the company will report the matter to the police and in cases of extremism or terrorism will work closely with the Local Authority and/or Hampshire Safeguarding Children's Board's.

Privacy and Monitoring

Basingstoke ITEC Limited reserves the right to monitor email, telephone and any other electronically mediated communications, whether stored or in transit, in line with the Regulation of Investigatory Powers Act (2000) and other relevant law. To support our duty of care to Learners on our programmes and more widely to protect all users of Basingstoke ITEC Limited ICT systems, there is software in place to monitor user activity and report potential areas of concern.

All websites visited by anyone on Basingstoke ITEC Limited premise is filtered to prevent access to malicious, illegal or inappropriate material. As a part of this process the pages visited are analysed to determine their content and categorised. Certain categories will be blocked by default for safeguarding, security or productivity reasons, any requests to unblock a site must be directed to the General Manager.

Communications and Social Networking

Basingstoke ITEC Limited recognises the role that social networking and other communication technologies holds within modern learner life and teaching practice. As such, these technologies are used within the company and made appropriately available to staff and learners within the company's ICT systems and networks.

In using these technologies, including email, mobile phones, social networking sites, chatrooms, video conferences and web cameras, Basingstoke ITEC Limited requires all users to adhere to the practices detailed within the ICT Acceptable Use Policy.

All staff members using social networking sites as tools through which to communicate with learners must only do so on a professional basis. Therefore, any groups that are set up under Basingstoke ITEC Limited name must only be done so using a Company email account, Revision 1 May 2018 and in line with the staff guidance detailed within the Safeguarding Policy. As such, staff must not become "social media friends" in a social capacity with learners within social networking or other virtual environments and must not share personal information with learners. All communications should be made in a manner that the professional position of the staff member(s) is not compromised and the relationship with the learner(s) remains appropriate in terms of professional boundaries.

Where a staff member chooses to join a group set up within a social networking site by a learner, the staff member must only do so using their designated company email account and having established that the nature and purpose of the group are appropriate in terms of the professional relationship.

Since social networking technologies are not Company systems, and the use of these technologies is optional, it is essential that where such systems are used by staff for the purposes of communication or discussion with learners, that appropriate steps are taken to ensure that any learner who chooses not to register with or use the technologies is not disadvantaged in their learning or overall learner experience.

Use of Images and Video

The use of images or photographs within Basingstoke ITEC Limited's learning and teaching and other activities is acceptable where there is no breach of copyright or other rights of another person. This includes images downloaded from the internet and images belonging to staff or learners.

Photographs of activities and people on Basingstoke ITEC Limited premise are considered carefully in terms of individual privacy and equality and diversity, and the consent of individuals pictured is sought prior to publication.

The potential risks of sharing personal images and photographs within social networking sites, and other areas of the internet for example are particularly relevant to e-safety. As such Basingstoke ITEC Limited will provide information, advice and training to learners and staff on these risks and steps that can be taken to protect personal images and photographs as well as other personal information.

Personal Data

Basingstoke ITEC Limited collects and stores personal data such as names, dates of birth, gender, ethnicity, email addresses, of learners and staff regularly in line with operational requirements. The Company has in place arrangements to ensure the secure and confidential storage of personal information, and that information is only shared appropriately and in line with Data Protection legislation and guidance.

All staff are required to gather, store and use learners' personal information appropriately.

Education and Training

While this Policy aims to ensure that ICT systems and resources are used appropriately and safely within Basingstoke ITEC Limited, it is impossible to eliminate all risks. However, the Company considers it to be an essential part of its approach to e-safety, for staff and learners to be equipped with the knowledge and skills to operate safely within the range of Revision 1 May 2018 technologies that is available. Through training and education, the Company will provide staff and learners with information and skills to enable them to identify risks independently and take steps to manage them effectively.

Incident Monitoring and Management

Basingstoke ITEC Limited will monitor the impact and effectiveness of this policy and will respond to any reported e-safety incident swiftly, and in line with other relevant policies and procedures such as the ICT Acceptable Use Policy, the Safeguarding Policy and the Prevent Policy. The Company will act immediately to prevent or minimise, as far as reasonably possible, any harm or further harm from occurring.

Learners will be made aware that should they wish to report an incident, they can do so to their Trainer Assessor, Mentor or any other member of staff in the first instance, where this is not possible then contact can be made directly with the Safeguarding Lead via email, post or telephone as detailed in the relevant policies. Where a member of staff wishes to report an incident, they will be able to do so through the General Manager.

Following any incident, Basingstoke ITEC Limited will take steps to address the matter thoroughly and appropriately and action may include the involvement of external agencies as necessary.

To ensure a fully appropriate and comprehensive response, serious incidents will be dealt with by the General Manager.

Responsibilities

- The General Manager has overall responsibility for the Policy and its implementation
- Basingstoke ITEC employ a third part who are responsible for managing the ICT infrastructure of the Company and the security of the data and user information held within Company systems

- The General Manager is responsible for managing the Safeguarding arrangements within the Company, including the Policy and Procedure and as such, is responsible for ensuring appropriate linkage between the E-Safety, Safeguarding and Prevent Policies
- The General Manager responsible for monitoring the impact of the policy and for coordinating responses to any e-safety incidents or concerns
- The Quality Lead is responsible for the co-ordination and delivery of learning materials relevant to E-Safety, for staff and learner use
- All staff members are responsible for ensuring that their professional behaviour and practice within their role is compliant with the content of this and other linked policies
- All staff must report any action by a member of the Basingstoke ITEC Limited community that incites people to commit acts of terrorism or violent extremism
- Learners are responsible for ensuring that their use of Company systems is compliant with the content of this and other linked policies