

ICT Acceptable Use Policy for Staff and Learners

Basingstoke ITEC Limited is committed to protecting staff and learners from illegal or damaging action by individuals, either knowingly or unknowingly.

As a user of IT services of Basingstoke ITEC Limited you have the right to use its computing services; that right places responsibilities on you as a user which are detailed below. If you misuse the computing facilities in a way that constitutes a breach or disregard of the following policy, you may also be in breach of other company policies.

Ignorance of this policy (or those it directs you to), and the responsibilities it places on you, is not an excuse in any situation where it is assessed that you have breached the policy and its requirements.

Staff and learners who connect their personal devices to Basingstoke ITEC Limited's network and the services available are particularly reminded that such use requires compliance with this policy.

Purpose

The purpose of this policy is to outline the acceptable and unacceptable use of computer equipment or on-line services owned by Basingstoke ITEC Limited, and acceptable or unacceptable general behaviour in areas of the company where there is ICT equipment.

These rules are in place to protect Basingstoke ITEC Limited's staff and learners. Inappropriate use exposes Basingstoke ITEC Limited and its stakeholders to risks including virus attacks, compromise of the network systems and services, and legal issues.

The management of information security and the use of computers at Basingstoke ITEC Limited are framed by UK legislation including:

- UK GDPR and the Data Protection Act 2018
- Counter-Terrorism and Security Act 2015
- Investigatory Powers Act (2016)
- Human Rights Act (1998)
- Computer Misuse Act (1990)
- PREVENT Duty Guidance (2015)
- The Protection of Freedoms Act 2012
- Safeguarding Vulnerable Groups Act 2006

Scope

This policy applies to all staff, board members, learners, contractors, consultants, temporaries and other workers at Basingstoke ITEC Limited, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Basingstoke ITEC Limited and to all equipment connected to the company's network. The use of Basingstoke ITEC Limited equipment and network are limited to staff, learners and authorised third parties only. Under no circumstances should any person not included in the list above be allowed to access the Basingstoke ITEC Limited network.

Disciplinary Procedures

Staff or learners who breach this policy may find themselves subject to the company's disciplinary procedures.

Individuals may also be subject to criminal proceedings. Basingstoke ITEC Limited reserves the right to take legal action against individuals who cause it to be involved in legal proceedings because of their violation of licensing agreements and/or other contraventions of this policy.

Definitions

For the purpose of this policy the term **computing services** refers to any ICT resource made available to you, any of the network services, applications or software products that you are provided access to and the network/data transport infrastructure that you use to access any of the services (including wired and wireless access to the internet).

The term **on-line services** include services provided and accessible (both wired and wireless) through individual accounts and passwords. Such services would include access to internet systems, included but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, internet browsing, and Microsoft 365 are the property of Basingstoke ITEC Limited. These systems are to be used for educational purposes in serving the interests of the organisation, and of our staff and learners during normal operations.

The term **devices** include but is not limited to: computers, laptops, tablets and smart phones.

The term **ICT facilities** encompasses computing services on-line services and devices as detailed above.

Definitions of Unacceptable

Usage Unacceptable use of company computers and network resources include, but are not limited to:

- Actions which cause physical damage to any ICT hardware, including cables, wiring, printers and the mouse
- Creating, displaying or transmitting material that is fraudulent or otherwise unlawful, likely to cause offence or inappropriate.
- Threatening, bullying, intimidating or harassing staff, learners or others
- Creating, accessing, transmitting or downloading inappropriate or extremist materials, as defined within the Prevent Policy. Basingstoke ITEC Limited has a statutory duty to take steps to prevent individuals from being drawn into extremism and terrorism, and a duty to alert and report any attempted access to, or dissemination of inappropriate material, which is either created, accessed, transmitted or downloaded
- Intellectual property rights infringement, including copyright, trademark, patent, design and moral rights.
- Defamation
- Unsolicited advertising, often referred to as spamming.

- Sending emails that purport to come from an individual other than the person sending the message.
- Attempting to use ICT facilities for bribery.
- Attempts to break into or damage computer systems or data held thereon.
- Actions or inactions which intentionally, or unintentionally, aid the distribution of computer viruses or other malicious software, e.g. use of equipment which is inadequately protected against viruses and spyware
- Attempts to access or actions intended to facilitate access to computer services, online services or devices for which the individual is not authorised.
- Using company network for unauthenticated access
- Unauthorised resale of company services or information
- Using ICT facilities for gambling
- Using the ICT facilities for carrying out any illegal trading activity
- Any other conduct which may discredit or harm the company, or its staff, learners or ICT facilities.

These restrictions should be taken to mean, for example that the following activities will normally be considered a breach of this policy:

- Interfering with data or settings in another person's network account
- The downloading, distributing, or storage of music, video, film or other material for which you do not hold a valid licence or other valid permission from the copyright holder
- The distribution or storage by any means of pirated software
- Circumventing of network access control
- Monitoring or intercepting of network traffic without permission
- Probing for the security weakness of systems by methods such as port-scanning without permission
- Public Wi-Fi should only be used where appropriate security controls are in place, such as VPN protection and secure authentication.
- Unauthorised use or transmission of the company and/or client information
- The use of portable media for copying unlicensed copyright software, music etc
- Allowing third party access to the ICT facilities, either on site or remotely over the internet, without prior authorisation from the ICT Systems Lead or the Chief Executive Officer.

Users must not deliberately visit, view, download, print, copy, forward or otherwise transmit any unlawful material or that which is likely to cause offence.

In the event of any use that could be regarded as giving rise to criminal proceedings, Basingstoke ITEC Limited may inform the police or other law enforcement agency. Other uses may be unacceptable in certain circumstances.

KEY PRINCIPLES

Authorisation

To use the ICT facilities of Basingstoke ITEC Limited, a person must first be properly registered. Registration to use Company services implies and is conditional upon acceptance of this Acceptable Use Policy as part of the Company regulations, for which a signature or electronic acknowledgement of acceptance is required. The lack of a signature does not exempt an individual from any obligation under this policy. The continuing use of the ICT facilities will be deemed to be acceptance by the user of the terms of this policy.

The registration procedure grants authorisation to use the core ICT facilities of the Company. Following registration, a username and password will be allocated to each individual user. Authorisation for other services may be requested to the ICT Systems Lead or Chief Executive Officer.

Any attempt to access, use or interfere with any user account or email address for which the user is not authorised, is prohibited and will be regarded as a disciplinary offence.

No one may use, or attempt to use, ICT facilities allocated to another person, except when explicitly authorised.

A user must take all reasonable precautions to protect the Company's resources (including the ICT facilities and the Company's information and data), their username and passwords. Initial passwords should be reset on the first day.

Purpose of Use

ICT facilities are provided primarily to facilitate a person's essential work as an employee or learner or another role within Basingstoke ITEC Limited. Company email addresses and associated Company email systems must be used for all company business. All staff must regularly read their company emails and delete unwanted or unnecessary emails at regular intervals.

Staff ICT Accounts have been allocated for use by the member of staff in connection with their job requirements. Learner ICT Accounts have been allocated for exclusive use by the learner in connection with their teaching, learning and assessment whilst at the Company.

Basingstoke ITEC Limited recognises that individuals may use the company email and internet for personal use, however this must be limited and in accordance with this policy.

Privacy and Monitoring

All allocated usernames, passwords and email addresses are for the exclusive use of the individual to whom they are allocated. The user is personally responsible and accountable for all activities carried out under their username. The password associated with a personal username must not be divulged to any other person. Passwords should not be recorded where they may be easily obtained and should be changed immediately if it is suspected that they have become known to another person.

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 Investigatory Powers Act (2016) and other relevant law.

Reasons for such monitoring include the need to:

- Prevent learners becoming radicalised and/or from being drawn into terrorism or extremist violence
- Safeguard learners and identify if there is a suspicion that a learner may be at risk, under threat or a victim of any activity or actions which may cause harm
- Establish the existence of fact
- Investigate or detect unauthorised use of the company's telecommunications systems and ensure compliance with this policy or other company policies
- Prevent breach of the law or investigate a suspected breach of the law, the company's policies and contracts
- Monitor standards and ensure effective quality control

In addition, Basingstoke ITEC Limited reserves the right for appropriate authorised staff to examine any data including personal data held on company systems.

When a learner or member of staff leaves the Company (either on completion of training or termination of employment) data held on any of the company's ICT facilities remains the property of the company. The Company is under no obligation to recover any data once a person has left the Company.

When a member of staff is away it may be necessary for appropriately authorised members of staff to access the absent member of staff's email account to deal with matters in their absence. This should be borne in mind when using the ICT facilities for personal reasons.

For operational reasons and for the continuing delivery of services, the Company has the right to access the network and email account of an individual after that person leaves.

Users of ICT facilities should be aware that the Company may conduct random monitoring of communications, regardless of whether the use is business or personal.

Where abuse is suspected (especially criminal activity and/or gross misconduct), Basingstoke ITEC Limited may conduct a more detailed investigation involving further monitoring and examination of stored data (including employee-deleted data) held on servers/disks/drives or other historical/archived data.

Where disclosure of information is requested by the police (or another law enforcement authority) the request where possible will be handled by the Chief Executive Officer.

Basingstoke ITEC Limited is committed to achieving an environment which provides equality of opportunity, and freedom from discrimination. Distributing material, which is offensive, obscene or abusive, may be illegal and may also contravene Company codes on harassment. No carrying out of unauthorised surveillance, audio and/or visual, of a learner, staff or member of the public on company premises is permitted.

No user shall interfere or attempt to interfere in any way with information belonging to or material prepared by another user. Similarly, no user shall make unauthorised copies of information belonging to another user. The same conventions of privacy apply to electronically held information as to that held on traditional media such as paper.

Users of services external to the Company are expected to abide by any policies, rules and codes of conduct applying to such services. Any breach of such policies, rules and codes of conduct may be regarded as a breach of this Acceptable Use Policy and be dealt with accordingly. The use of Company credentials to gain unauthorised access to the facilities of any other organisation is similarly prohibited.

Copyright Compliance

All users must abide by laws relating to copyright and therefore must not download, copy or otherwise re-produce material for which they have not obtained permission from the relevant copyright owner. If such material is required for any purpose e.g. teaching or research, then copyright permission must be obtained and documented before such material is used.

Employees and Learners are reminded that the Company treats plagiarism very seriously and will investigate any allegation i.e. the intentional use of other people's material without attribution.

Responsibilities

1. This policy is the responsibility of the Chief Executive Officer
2. The ICT Systems Lead is responsible installation and maintenance of all ICT facilities within Basingstoke ITEC Limited and the logging and monitoring of the security systems in place
3. The Company Quality Lead is responsible for the implementation and monitoring of the policy including copyright compliance monitoring of teaching and learning resources
4. All persons identified within section 2 have a responsibility to comply with this policy
5. Any suspected breach of this policy should be reported to the Chief Executive Officer, who will determine the appropriate action within the company's disciplinary framework. Basingstoke ITEC Limited reserves the right to audit and/or suspend without notice any account pending an enquiry. Where necessary, this will include the right to intercept communications

This policy is not exhaustive and inevitably new social and technical developments will lead to further uses, which are not fully covered here at present. Where there is any doubt the matter should be raised with ICT Systems Lead, who will ensure that all questions are dealt with at the appropriate level within the Company.

Summary

You must not:

- Allow other people to use your account
- Download or access illegal software onto a workstation
- Download or copy any software from the company network onto portable media etc
- Download, copy or remove from the system and/or client information without permission
- Upload your own personal software packages onto company workstations
- Access offensive or abusive material
- Send abusive or inappropriate emails
- Access inappropriate websites
- Interfere with other users work
- Access, transmit or download inappropriate or extremist materials, as defined in the Prevent Policy
- Photograph or record members of staff or learners without their permission Use software designed to unblock sites
- Use online gambling sites
- Abuse equipment

Company computers are provided primarily for company work or purposes of education. However, you may use the equipment for personal use providing you do not breach the Acceptable Use Policy.

If you use the company equipment for personal use, you should note the following:

- Conducting any financial transaction on shared equipment carries a very high risk. Your personal data may not be safe
- This Acceptable Use Policy applies to both wired and wireless access and use of network on your own devices or on Company equipment
- To use the ICT facilities of the Company a person must first be properly registered
- Registration to use Company services implies and is conditional upon acceptance of this Acceptable Use Policy
- The continuing use of the ICT facilities will constitute an acceptance of the terms of this policy by the user