Computer and Internet Use – Our Policy

Version: 3.5; effective from January 2025
Policy Summary: The Computer and Internet policy document is a summary of the Cheynes Training approach to preventing misuse of computer and internet resources

---

Introduction

Cheynes Training provides access to various online training and assessment resources using the Internet. These resources are available to enhance learning and help achieve positive learning outcomes for all those involved in our programmes. We encourage all users to become familiar with the use of Information technology and to use the internet in a safe and secure way.

The company has invested in a secure networking IT structure controlled via a dedicated server. We use the latest in broadband/WIFI and computing software systems to ensure the use of IT/Databases is protected to a high standard including Multi Factor Authentication. This includes a server firewall and the latest antivirus/spamware software which is updated on a regular basis. CT also buys into a dedicated IT support from one of the leading IT Companies in the UK, this includes all technical support, 24/7 monitoring of server including alerts to any misuse or malfunction of network. Regular weekly updates are applied to our systems to ensure the latest work/security patches are employed. The company has an in-house IT Systems Administrator who carries out regular checks and provides technical support as and when required in conjunction with our IT support company when necessary. All networking passwords/WIFI codes are confidential to Cheynes Training. Cheynes Training are also Cyber Essential certified, and systems are checked yearly to ensure compliance and certification.

As a responsible company, we expect all users, especially those under the age of 18 and others who may be vulnerable, to respect and follow the guidelines set out below which are based on common sense and UK government legislation. For the benefit of everyone, all users are expected to observe the following:

1 Use of Computer Equipment - Learner

All users must respect the computer equipment with which they have been provided and understand that the use of this equipment is designed to help with studies. All users must only use computers for the purpose directed by the designated person in charge and users must not to play games, surf the internet or use any other software without explicit permission. Company WIFI codes are not accessible by any learner.

- **DO NOT** use computers unless permission has been given, and use is supervised.
- **DO NOT** tamper with the computer system.
- **DO NOT** use pen drives or removable media without specific permission.
- **DO NOT** touch the monitors with fingers or any other object, for example, pens.
- **DO NOT** use monitors or keyboards to rest books, papers and folders on.
- **DO NOT** swap equipment from one computer to another.
- **DO NOT** download any files from the internet without specific permission
- **DO NOT** share passwords with anyone.

Please report all equipment faults to your tutor/assessor immediately.

2 Use of Computer Equipment - Employee

All users must respect the computer equipment with which they have been provided and understand that the use of this equipment is solely for business purposes. Allocation of user access privileges is granted by the IT Administrator and is based on the user's role and the data they are required to access.

3 Home and mobile working

IT equipment used for home working must be connected to a secure network domain and network access is via VPN set up securely by the IT Administrator.

4 Printing

Cheynes Training provides printing facilities for users to obtain printouts of their work. Users are expected to use the printers for education purposes only and to keep paper and toner wastage to a minimum.

- Before printing, proofread, spell check, and print preview your document.
- Print the document only when completely satisfied with the final product.
- If printing information from websites, please ensure that you have copied the relevant information to a document and are not wasting paper by printing adverts and unneeded graphics and information from websites.

5 Use of the Internet

Dangers exist on the internet from individuals who may seek to harm young people under the age of 18 and others who may be vulnerable. Dangers also exist from downloading corrupted files or viruses that may 'infect' the computer system.

Why do we use the internet?

Tutors, assessors and learners on training programmes use the internet to locate information, send electronic mail, browse documents or images from various sites including our own, to locate and use files on our own system and to access our client information system.

Some of the ways we use the internet:

- Electronic mail
- Accessing information
- Electronic publishing
- Collaboration with others
- Projects and assignments
- Support and in-service training
- Technical support
- Online booking

Individual users of our computer systems are responsible for their behaviour and are expected to adhere to the following acceptable use policy.

Continued

6 Extremism and Radicalisation

People with extreme views regularly use the internet and may attempt to groom young people and others who may be vulnerable. Their aim is to radicalise and draw others into extremism by sharing videos and other material. It is the responsibility of all those involved in apprenticeship programmes, including employers, directors, senior managers, teachers, assessors, learners, and contractors, to have due regard for the need to prevent people from being radicalised, drawn into extremism and, in the worst situation, terrorism by the unintentional access to extreme websites.

The ability to connect to other computers through a network or via the internet does not imply a right to connect to those systems or to make use of those systems unless authorised to do so.

Accessing social media sites such as Facebook or Instagram are expressly forbidden.

The use of computer equipment to make downloads or make copies of computer programmes, music or video is strictly prohibited and is viewed as gross misconduct.

7 Secure Transmission of Personal Data on Paper or Electronically

All sensitive personal data sent by Cheynes Training is transmitted via our secure information sharing portal called Huddle. Cheynes Training strongly advises against sending any sensitive or confidential information by courier or special delivery services; however, if this is unavoidable, the sender assumes all risks associated with delivery. The package should be clearly labeled as confidential and intended for the addressee only. Cheynes Training disclaims any liability for personal information sent via these methods if it is lost or compromised during transit.

8 Email

The use of Cheynes Training computer equipment for private email is not permitted. In serious cases involving material of a defamatory, libellous, obscene, offensive, racist or sexual nature, the matter will be treated as gross misconduct.

You are advised that all email and internet activity is monitored, and Cheynes Training reserves the right to access any email at any time.

9 Copyright

All users are expected to respect and adhere to the law regarding copyright and the use of copyright materials.

You must obtain permission from the Cheynes Training IT Administrator before copying files from another user. Copying files or passwords belonging to another user or author without their permission may constitute plagiarism or theft.

10 IT System Care

Cheynes Training has in place a complete System Care IT support solution contract outsourced with TSG (a high-end information technology company), TSG continuously monitors our IT network for any issues. TSG also provides day to day unlimited access to technical support service to deal with any issues that may arise, this ensures that critical systems failures can be resolved with little or no business disruption.

The Cheynes Training on-site server and internet access devices have a high standard of protection including network monitoring, updated firewalls and malware, network and device cryptography and specialised in cloud-based email management for Microsoft Exchange and Microsoft Office 365, this includes security, archiving, and continuity services to protect business mail.

11 Incident Management

Data systems used by Cheynes Training are cloud based so that in the event of an incident that could lead to loss of or disruption to Cheynes Training operations, services or functions, the Cheynes training incident management software can identify and correct hazards to prevent a future re-occurrence.

12 Data

Cheynes Training uses a cloud-based learner management system called PICS which is hosted by One Advanced who are fully compliant with the Data Protection Act.

13 Breach of rules

Breaches of this policy may result in users being excluded from using the company computer equipment except under very strict supervision and/or other disciplinary action. Failure to comply with this policy will be dealt with severely and may be regarded as gross misconduct.

14 Related Policies

The Cheynes Training Computer and Internet Use Policy should be read in conjunction with the following related policies, each of which are available for downloading from the Cheynes Training website:

- Safeguarding Policy
- Anti-harassment Policy
- Complaints and Dispute Resolution Policy
- Equality, Diversity and Inclusion Policy

This policy will be kept under review and updated every two years or as required.

Last Review: January 2025
Next Review: January 2027

Melanie Mitchell,
Managing Director.
January 2025