# Using Technology for Learning

## ***Why do we need an Acceptable Use Policy?***

This policy is written to help you use Information technology (computers, tablets and mobile devices) in a safe way that helps and enhances how you learn. It aims to keep all apprentices, learners and service users safe while using technology e.g. from online bullying, disclosure and to keep your details and information safe.

Information Technology and devices such as computers, tablets and mobile devices are very useful tools in all forms of learning so we want to make sure that our apprentices, learners and all service users agree to use them in a safe and responsible way. When you sign your enrolment form, learner agreement or apprenticeship contract you are also saying that you agree to the details contained within this policy. Once you have agreed you will be given a username and password to access our online systems and resources.

**This is a list of things all apprentices, learners and service users must agree to; if you ignore of breach the conditions set out below, you could be stopped from accessing and using our information technology systems and learning platforms.**

**Please read this list carefully** as when you sign your enrolment form you are agreeing to this policy. If you do not understand anything please ask your tutor/assessor/manager to explain.

We expect all our apprentices, learners and other service users to respect the safety and security others. Apprentices, learners and other service users should not use their mobile phone, or any other form of technology, in a manner that is likely to bring the centre into disrepute, cause offence or risk the safety of a child, young person or vulnerable adult.

If you are upset by any calls, texts, images, videos etc. please report it **immediately to a member of staff** in the centre**.**

## 1. Equipment

### 1.1 Vandalism

You must not do anything to harm or damage any equipment or information that is part of the centre ICT facilities. This is covered by the Computer Misuse Act 1990 (see Glossary). This includes:

- Damaging computers, display screen equipment, printers, keyboards, mice or other equipment
- Changing or removing software
- Creating or uploading computer viruses

- Removing files on purpose

If information technology resources and equipment is damaged, other learners cannot use them.

### 1.2 Bringing and using your own Device

Any apprentice, learner or other service users can bring and use their own device to support their learning.

- Please ensure your device is fully charged and used in compliance with the terms set out in this policy
- The Council accepts no liability whatsoever, under any circumstances for your device or use thereof
- Use of your own device is entirely are the users own risk, without exception

### 1.3 Use of plug in devices

Only use portable memory cards, USB memory stick or other plug in devices once you have spoken to you tutor/assessor/member of staff to verify that they are safe to use.

### 1.4 Printers, Paper and Ink

Printers, photocopiers and scanners should be used for your course work only. Always check before you print to make sure you only print what you need, if you are unsure please ask your tutor.

All our printers keep records of what you print so if you print anything that is not for your course or you print something that would upset other learners your tutor or the centre manager will:

- Provide you with a reminder concerning acceptable use
- Limit your access to print and other facilities
- In some cases staff may contact the police

### 1.5 Data Security and Retention

All your work is stored on the system and is copied and saved for two weeks. If you accidentally delete files, please inform your tutor *immediately,* so that it can be recovered. It is not possible to recover files that were deleted more than 2 weeks previously.

## 2. Internet, Email and Wi-Fi

### 2.1 Derbyshire Guest Wi-Fi

All our centres have guest Wi-Fi connectivity, which can be accessed by all our apprentices, learners and other service users. You must accept the Wi-Fi terms and conditions before you connect to the Wi-Fi.

### 2.2 Internet management

We use internet filtering which helps to stop offensive or illegal content being accessed on our devices or in our centres. However we cannot make sure that all material is filtered. If you find any websites that worry you, **please report it to a member of staff straight away.**

### 2.3 Acceptable Use of the Internet

**All Internet access is logged and actively monitored** and it is stored. Usage reports are used and can be provided to any member of staff, if they suspect suspicious activity.

Use of the Internet should be within the following guidelines:

- The Internet must not be used to download, send, print, display or send material that would cause offence or break the law.
- Do not access Internet chat sites or forums or social media site such as WhatsApp unless this is part of your course.
- Protect your personal information. Never give or enter personal information on a website, especially your home address, your mobile number or passwords.
- Do not access online gaming sites; remember that your use of the Internet is for learning purposes only.
- Do not download or install software from the Internet.
- Do not use the Internet to shop online unless this is part of your course.
- Take care when printing pages directly from a website; web pages are often not properly formatted for printing and this may cause a lot of waste, always use the print preview option and select the required pages. If you wish to use content from websites, consider using the copy and paste facility to move it into another application, copyright permitting.

### 2.4 Email

You are expected to use email in a responsible manner. The sending or receiving of messages that contain any material that is of a sexist, racist, unethical or illegal nature, and/or likely to cause offence, should not take place.

Remember when sending an email to:

- **Be polite** - never send or encourage others to send abusive messages
- **Use appropriate language** – remember what you say and do can be viewed by others. Never swear or use any other inappropriate language
- **Do not reveal any personal information about yourself or anyone else**, especially home addresses, personal telephone numbers,

usernames or passwords. Remember that email is not guaranteed to be private

- **Think about the file size of an attachment -** files exceeding 1MB in size are generally considered to be too big and you should think about using another way to transfer large files
- **Do not download or open file attachments unless you are certain they are safe and from someone you know** - file attachments may contain viruses that may cause damage to the centre network

### 3.0 External Services

We have a number of services that you can access outside the centre, using any device with an Internet connection. You should only use these facilities for learning. Your tutor or assessor will let you know what is available.

### 3.1 Learning Pool, OneFile, BKSB and Office 365 sites

These are internet sites that can provide remote access to files, learning materials and resources via the Internet.

They are all closely checked and if they are misused access will be reviewed and may be removed. When using Learning Pool, OneFile, BKSB and Office 365 sites please follow these guidelines.

- All these sites are provided for use by staff and learners only.
- They are all supported by external companies and we cannot guarantee their service availability or quality.

## 4.0 Privacy and Data Protection

### 4.1 Passwords

- **Never** share your password with anyone else or ask others for their password.
- When choosing a password, use a strong password - at least 12 characters with upper and lower case letters, numbers and special characters like asterisks or currency symbols
- Don't choose a password based on any personal data such as your name, age, or your address. Avoid using words (English or otherwise) as well as any proper names, names of television shows, keyboard sequence or anything else that can be easily guessed or identified.
- We advise using a passphrase; your tutor/assessor can help you with this
- If you forget your password, tell your tutor immediately
- If you think that someone else knows your password, then **change it immediately** and tell a member of staff

### 4.2 Security

- **Never** try to access files or programs which you have not been given access to

- You should report any security concerns immediately to a member of staff
- If you are identified as a security risk to the centre ICT facilities, you will not be allowed to use them

### 4.3 Storage and Safe Transfer of Personal Data

- We hold information on all learners and, in doing so, we must follow the requirements of General Data Protection Regulation 2016 (see Glossary). This means that data held about you can only be used for agreed reasons and all data will be used as permitted under the terms of the General Data Protection Regulation 2016.
- We will make sure that any personal data or sensitive information, sent over the internet or email, will be secured.

## 5.0 Service

We do our best to ensure that the IT systems and networks are working correctly; the service will not be responsible for any damages or loss as a result of faults, malfunctions or routine maintenance. Use of any information obtained in the centre ICT system is at your own risk. We deny any responsibility for the accuracy of information obtained whilst using the ICT systems and networks.

# Glossary

## Computer Misuse Act

The Computer Misuse Act makes it an offence for anyone to:

- have unauthorised access to computer material, e.g., if you find out, or guess a fellow learner's password and use it
- have unauthorised access, to deliberately commit an unlawful act, e.g., if you guess a fellow learner's password and access their learning account, without permission
- make unauthorised changes to computer material, e.g., if you change the desk-top set up on your computer, or introduce a virus deliberately to the centre's network system.

## General Data Protection Regulation 2016 (GDPR)

The General Data Protection Regulation 2016 ensures that information, held about you, is used for specific purposes only. These rules apply to everyone in the service, including teaching staff, support staff, volunteers and governors.

GDPR covers the collection, storing, editing, retrieving, disclosure, archiving and destruction of data held about individuals in the service. The Act not only applies to paper files, it also applies to electronic files.

The Principles of GDPR state that data must be:

- fairly and lawfully processed
- processed for limited purposes
- adequate, relevant and not excessive
- accurate and up to date
- kept no longer than necessary
- processed in accordance with data subject's rights
- secure
- not transferred to other countries, without adequate provision.

## RIPA – Regulation of Investigatory Powers Act 2002

If a request for authorised access is made to the service, we will provide the appropriate access to your ICT records and files. The Act legislates for using methods of surveillance and information gathering to help the prevention of crime, including terrorism. RIPA makes provision for the:

- interception of communications
- acquisition and disclosure of data relating to communications
- carrying out of surveillance
- use of covert human intelligence sources
- access to electronic data protected by encryption or passwords.