Acceptable Use of Technologies Policy

IT Services

Version:	V3
Name of author:	Executive Director of ICT
Name of responsible manager:	Executive Director of ICT
Date issued:	November 2014
Review date:	November 2018
Next review date	November 2019

Introduction

Purpose

This Acceptable Use of Technologies Policy (AUTP) applies without exception to all users of ICT facilities and equipment within the Grimsby Institute Group (the Group). This includes staff, students and any visitors who have been provided with temporary access privileges.

The purpose of this policy is to provide guidance on the use of network resources which includes the use of any Group Learning Space (internal or cloud based, the internet, e-mail, instant messaging, social media, media publications, file transmission and voice/data communications.

Scope

The policy applies to activities taking place in any location where access to and the use of any of the Group systems and/or equipment takes place, e.g. laptop computers at home; remote access to any of the Group Learning Space and/or networked resources.

The policy also covers the use of personally owned PCs on the Group premises and which are connected to any of the Group's network.

All users will be deemed to be familiar with and bound by this AUTP. A copy of this policy can be found on the Group's intranet zone. Paper copy can also be made available upon request.

Change

This policy is maintained by the Group's Computer Services Department. Requests to change the policy should be made to the Executive Director of ICT and Learning Technology in writing. All changes will need to be approved by the Executive Director of ICT and Learning Technology and the Group's Chief Executive.

Authorisation

In order to use ICT facilities at the Group a person must have been issued staff, learner or guest access to the network. Use of the Group facilities will be deemed to be acceptance of the terms and conditions of this policy.

It is expected that all users will adhere to group password policy and guidelines, data protection policies in addition to all relevant regulatory and legal requirements.

Privacy and Monitoring

The Group's IT Services department reserve the right to monitor email, telephone and any other electronically-mediated communications, whether stored or in transit, in line with relevant legislation.

All users of the Group facilities or equipment expressly waiver any right of privacy and therefore should have no expectations of privacy in anything they create, store, send or receive using the Group's ICT systems and equipment.

If you are using your own device which is connected to the Group's network (wired or wireless) you

expressly waiver any right of privacy and therefore should have no expectations of privacy in anything you create, store, send or receive.

Reasons for such monitoring include the need to:

- Establish the existence of facts (e.g. to provide evidence of commercial transactions in cases of disputes);
- Investigate or detect unauthorised use of group telecommunications systems and ensure compliance with this policy or other Group policies;
- Ensure operational effectiveness of services (e.g. to detect viruses or other threats to the systems);
- Prevent breach of the law or investigate a suspected breach of the law, the Group polices or contracts;
- Monitor standards and ensure effective quality control.

Monitoring may involve:

- Examining the number and frequency of emails;
- Viewing sent or received emails from a particular mailbox or stored on any server;
- Examining logs of ICT facility usage;
- Monitoring the amount of time spent on the Internet;
- Internet sites visited and information downloaded.

Where abuse is suspected a more detailed investigation involving further monitoring and examination of stored data may be undertaken.

Where disclosure of information is requested by the police, (or another law enforcement authority) the request should be directed to the Executive Director of ICT and Learning Technology or other designated staff member.

The Group staff that have access to personal data, (as defined under the Data Protection Act 1998) are responsible for ensuring that such data is not made available to unauthorised individuals and that the security of all systems used to access and manage this data is not compromised.

The Group's IT Services maintain the right to access the Group email account of staff members after termination of employment for operational reasons and for the continuing delivery of services.

Definitions of Unacceptable Usage

Unacceptable use of computers and network resources may be summarised as:

- Viewing, creating, displaying or transmitting material that is fraudulent or otherwise unlawful or inappropriate.
- Threatening, intimidating or harassing employees and students including any message that could constitute bullying or harassment, e.g. on the grounds of sex, race, disability, religion or belief, sexual orientation or age.
- Using obscene, profane or abusive language.
- Using language that could be calculated to incite hatred against any ethnic, religious or other minority group
- Intellectual property rights infringement, including copyright, trademark, patent, design and moral rights
- Defamation (genuine scholarly criticism is permitted)
- Unsolicited advertising often referred to as "spamming"
- Sending emails that purport to come from an individual other than the person actually sending the message using, e.g. a forged address

- Attempts to break into or damage computer systems or data held thereon referred to as "hacking"
- Actions or inactions which intentionally or unintentionally cause a breach of the Group's ICT Security including but not limited to:
    - Aiding the distribution of computer viruses or other malicious software.
    - Attempts to access or actions intended to facilitate access to computers for which the individual is not authorised
    - Using the network for unauthenticated access
    - The introduction or connection of unauthorised hardware to the Group's IT Network infrastructure
- Using the ICT facilities to conduct personal commercial business or trading
- Spending unreasonable amount on time on non-work related sites e.g. Social Media websites.

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

- Viewing, downloading, distribution, or storage of music, video, film or other material, for which you do not hold a valid license or other valid permission form the copyright holder
- Distribution or storage by any means of pirated software
- Connecting an unauthorised device to the network, i.e. one that has not been configured to comply with this policy and any other relevant regulations and guidelines relating to security, purchasing policy, and acceptable use
- Circumvention of network access control
- Monitoring or interception of network traffic, without permission
- Probing for the security weaknesses of systems by methods such as port-scanning, without permission
- Associating any device to network Access Points, including wireless, to which you are not authorised
- Non-academic/non-business related activities which generate heavy network traffic, especially those which interfere with others' legitimate use of ICT services or which incur financial costs
- Excessive use of resources such as file store, leading to a denial of service to others, especially when compounded by not responding to requests for action
- Frivolous use of ICT suites, especially where such activities interfere with others' legitimate use of ICT services
- Use of CDs, DVDs, and other storage devices for the purpose of copying unlicensed copyright software, music, etc.
- Copying of other peoples' website material without the express permission of the copyright holder
- Use of peer-to-peer and related applications for non-business or non-educational purposes. These include, but are not limited to, Ares, BitTorrent, Direct Connect, Morpheus, KaZaA

Staff, learners, and visitors should consider the spirit of the Group's Ethos when working on The Group systems. Any conduct which may discredit or harm the Group, its staff or the ICT facilities or can otherwise be considered intentionally unethical is deemed unacceptable.

Incidents of misuse will be dealt with by the Group in accordance or be subject to the disciplinary procedures outlined in the terms and conditions of employment (staff) and admissions policy (learners). The appropriate level of sanctions will be applied as determined by the nature of the

reported misuse.

Group Network Use

The Group network is not to be used for any of the following purposes:

- Viewing, creating, storing, transmitting or deliberate receipt (other than for properly supervised and lawful research purposes) of any offensive, obscene or indecent images (including pseudo images), data or other material, or any data capable of being resolved into obscene, unlawful or indecent images or material;
- Viewing, creating, storing or transmitting of material which causes, or is likely to cause annoyance, revulsion or needless anxiety to the Group, its staff, learners, visitors or any third party.
- Viewing, creation or transmission of defamatory abusive or other unlawful material in respect of the Group, its staff, learners, visitors or any third party;
- Viewing, storage or transmission of material in such manner that it infringes the copyright of the Group, another person or organisation or which discloses confidential or sensitive information or data relating to the Group, its staff, learners, visitors or any third party;
    a. transmission of unsolicited commercial or advertising material
    b. any other act which is considered unlawful in any country where the network is being accessed
    c. deliberate activities with any of the following characteristics:
        i. wasting staff effort or networked resources, including the effort of staff involved in the support of these services, including but not limited to
        ii. corrupting or destroying the Group's or other users' data
        iii. manipulating and altering assessments, grades or transcripts
        iv. accessing and copying files of other users in order to obtain an improper advantage
        v. violating the privacy of the Group or other users
    d. disrupting the work of other users; using the Group network in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment)
    e. continuing to use an item of networking software or hardware after a request that use cease because it is causing disruption to the correct functioning of the Group network
    f. other misuse of Group network or networked resources, such as the introduction of viruses, extracting material of others and passing it off as one's own, manipulating material of the Group or others to one's own advantage, whether pecuniary or otherwise
- Where the Group network is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of the Group network.
- All the provisions of the Acceptable Use Policy of the Joint Academic NETwork ("JANET") apply to users of the Group network in addition to the provisions herein

- Users are not permitted to access the Group network on behalf of third parties without prior written agreement of the Group
- It is beyond the resources and ability of the Group to monitor all activities. However, where there is sound reason to suspect unacceptable use as defined above, the Group reserves the right to inspect a user's material and use history, including email messages, and at its sole discretion block or edit such material as it sees fit. Furthermore, from time to time, the Group may implement technical measures to monitor activity on the Group network to ensure compliance with the requirements of this policy and to carry out tests for research purposes.
- Acceptance of the right of the Group to take steps to prevent suspected misuse is a condition of access to the Group network.
- Any external organisation having a direct link into the Group network must take all reasonable steps to ensure compliance with the requirements of this Policy and to ensure that unacceptable use of the Group network does not occur. The external organisation must also accept responsibility for adequately informing its own users of the conditions of use of the Group network
- Where necessary, and at the sole discretion of the Group, access by an individual or organisation may be withdrawn, either temporarily or indefinitely.
- In the event of misuse of the Group network, the Group reserves the right to exclude access to any external organisation, or employee, or learner and in the case of:
    a. misuse by an employee of the Group, to proceed against that employee under the Group's disciplinary procedures for employees and
    b. misuse by a student, to proceed against that student in accordance with the Group's Learner Disciplinary Procedures.
- Individuals must not share the passwords for any of their Group accounts. Account owners are held responsible for all activities and content associated with their accounts. Failure to conform to these requirements may lead to the suspension of account privileges or other actions as provided by the appropriate Group policy. If an individual believes that someone else is accessing their account, they must report this immediately to the IT Services itservices@grimsby.ac.uk.

Password Guidelines

Passwords are an important means of protecting user's privacy from unauthorized access. With minimal effort, users can greatly increase the effort required by an unauthorised user to compromise information and/or privacy. The following points relate to password selection and use on all Group ICT Systems.

A password is defined as a secret series of alpha-numeric characters that allow a user to access a computer, program, file or other ICT resource.

- Passwords should not be shared. Users may receive phone calls from people claiming to be Group IT employees asking for a user's password. Users should never give their password to anyone under any circumstances. Users are responsible for all activity on their account.

- Users should log out of or otherwise lock computers or other resources when finished using them.

- Passwords should be at least eight characters long and contain at least one non-letter (a-z, A-Z) character. Passwords should not be the same as a users' logon ID, and should not be a word found in a dictionary.

- Passwords should not be written down in insecure locations. Insecure locations include, but are not limited to, under the system keyboard, system monitor or desk. If a password must be written down, it should be kept in a secure location.

- The system will automatically ask you to change your password(s) regularly

- Most incidents of computer "hacking" or other forms of uninvited intrusions are the result of poor password selection or protection. Group IT Services personnel may occasionally audit passwords as part of a security exercise. If a password is found that does not meet requirements for complexity and length, the user will be notified and asked to change their password to meet the requirements.

Device/Laptop security guidelines

This section provides recommendation for adoption by the Grimsby Institute Group (Group) where laptop computers and other mobile devices are used. The policy is equally applicable to contractors, services providers and other organisations or agencies that use laptop computers to process Grimsby Institute information in the performance of their duties.

Introduction

- Laptop computers taken outside secure Group environments are subject to special security risks: they may be lost or stolen and may be exposed to unauthorised access or tampering. Laptops taken abroad may also be at risk, for example confiscated by police or customs officials.

- Laptop loss will mean not only the loss of availability of the device and its data, but may also lead to the disclosure of sensitive information – such as student assessment data. This loss of confidentiality, and potentially integrity, will often be considered more serious than the loss of the physical asset.

- Where possible data should not be stored on the laptop but rather on the network storage systems provided.

- If quantities of Group data are held on a single laptop (or any other storage medium) risk assessments must consider the impacts of loss of all the data. Note that deleted files should be assumed to persist on the laptop's hard disk.

Key points:

- Traditional password protection on a laptop offers limited defense against a determined attacker because the attacker has unconstrained access to the physical device. Modern complex password techniques offer more protection which must therefore be used.

- The physical security controls that are possible within the Group buildings environment are not available outside of that environment; therefore, if procedural and personal controls of the laptop are breached the only effective technical measure that can be applied is cryptography.

The preferred cryptography product is TrueCrypt. It is important that this product be used correctly in accordance with defined procedures, in particular the password and any token must be kept separate from the laptop; these are effectively the encryption key. Data is therefore only protected by encryption when the laptop is powered off and not in normal use. From time to time we may consider using other encryption technologies.

- Unauthorised access and tampering to a laptop, particularly if there are repeated opportunities for access, may:

• lead to continuing (and undetected) compromise of information on the laptop itself

• undermine security measures (including the encryption); intended to protect information on the laptop in the event of loss or theft; and

• lead to compromise systems to which the laptop is connected, for example, a networked system that is accessed from the laptop.

• The impact of a breach of laptop security may therefore extend far more widely than the laptop itself.

Security of equipment off-premises

• Security should be applied to off-site equipment taking into account the different risks of working outside the organisation's premises

• Regardless of ownership, the use of any information processing equipment outside the organisation's premises should be authorised by management

• Security risks, e.g. of damage, theft or eavesdropping, may vary considerably between locations and should be taken into account in determining the most appropriate controls.

Mobile computing and communications

• A formal policy should be in place, and appropriate security measures should be adopted to protect against the risks of using mobile computing and communication facilities

• Special care should be taken to ensure that business information is not compromised. The mobile computing policy should take in to account the risks of working with mobile computing equipment in unprotected environments

• The mobile computing policy should include the requirements for physical protection, access controls, cryptographic techniques, back-ups, and virus protection. This policy should also include rules and advice on connecting mobile facilities to networks and guidance on the use of these facilities in public places.

Security measures

• Laptops should be secured to a desk or other appropriate point if left unattended using an appropriate locking mechanism

• Ensure that laptops or mobile devices are not left unattended when working off-site

• When travelling and not in use, ensure that laptops are stored securely out of sight. For example, when travelling by car, ensure laptops are locked in the boot. Laptops left on display and unattended will inevitably attract attention and are likely to be stolen.

• It is good practice to carry laptops in protective anonymous bags or cases (i.e. those without manufacturer logos on them) when not in use

• Full disk encryption (TrueCrypt) should be used with laptops whenever possible

Other good practice security measures

• Do not leave laptops or mobile devices unattended in car boots overnight

• Do not leave laptops unattended in insecure areas, for example meeting rooms next to areas of public access, and hotel rooms where others may have access. Make use of room locks and lockable storage facilities where available

• Be aware of the potential for opportunist or targeted theft of laptop bags in busy public places including airports, train stations, hotel lobbies, exhibition halls etc. and on public transport e.g. buses and trains

• When travelling, avoid placing laptops in locations where they could be easily forgotten or left behind e.g. overhead racks and taxi boots

• Be aware that the use of laptops in public places will likely draw the attention of those in the vicinity. It is possible that information viewed on a laptop screen could lead to the unauthorised disclosure of that information being processed.

Legal constraints

Software may not be copied, installed, or used on the Group's IT equipment except when and as permitted by the owner of the software and by law and with agreement from the Group IT Services department. The department will properly license software and strictly adhere to all licensing provisions, including installation, use, copying, number of simultaneous users, and terms of the license

It is up to the user to check the terms and conditions of any license for the use of the software or information and to abide by them. Software provided by the Group's IT Services department may only be used as part of the user's duties as an employee or student or for educational purposes.

The user must abide by all the licensing agreements for software entered into the by the Group with other parties, noting that the right to use any such software outside the Group premises will cease when an individual leaves the institution. Any software on a privately owned computer that has been licensed under the Group's agreement must then be removed from it, as well as any Group owned data.

The user must comply with all the relevant legislation and legal precedent, including the provisions of the following Acts of Parliament, or any re-enactment thereof:

- Copyright, Designs and Patents Act 1988;
- Malicious Communications Act 1988;
- Computer Misuse Act 1990;
- Criminal Justice and Public Order Act 1994;
- Trade Marks Act 1994;
- Data Protection Act 1998;
- Human Rights Act 1998;
- Regulation of Investigatory Powers Act 2000;
- Freedom of Information Act 2000;
- Communications Act 2003;
- Criminal Justice and Immigration Act 2008.

Any breach of the above legislation or related polices is considered to be an offence and in that event, the Group' s disciplinary procedures will apply.

For further information, please contact IT Services: itservices@grimsby.ac.uk

Use of Biometrics

Objective

The objective of this policy is to ensure an efficient way of approach to the collection and handling of biometric information by the Group. Our actions will be consistent with Data Protection Act 1998.

Biometric Information

Biometrics authentication is the automatic recognition of a living being using suitable body characteristics. By measuring an individual's physical features in an authentication inquiry and comparing this data with stored biometric reference data, the identity of a specific user is determined. Once the fingerprint has been scanned the next stage in the Biometric process is authentication in order to grant access to appropriate application and/or facilities. A biometric feature is saved on to a database. Certain data will be held on the system to enable accurate operation. This will include the name, class (for learners), photo, account balance and meal entitlement.

Purpose of Collection of Biometric Information

The purpose of the use of biometrics is to support the cashless catering (where implemented), access to printing and photocopying, registration and loan of books from the library and registration of students. Each user needs to only register once, reducing the need for various applications requiring identification at several areas. With a biometric system, users cannot borrow or steal personal information from each other, reducing the opportunities for bullying. Queues are reduced, because the identification of users is speeded up.

Handling of Biometric Information

The biometric database is stored on the Group's own computer. This data will be handled under the guidelines of the Data Protection Act 1998 and only used by the Group and those directly involved with the implementation of the system.

Appendices - Guidance documents

To support in determining how to apply the AUTP and to adapt to your own environment a series of Guidance documents are provided for consideration.

The Guidance documents cover:

Appendix 1 - Legal constraints - references
Appendix 2 - Use of technologies around The Group
Appendix 3 - Sample Acceptable Use of Technologies Agreements: The Group Staff

Appendix 1

Legal constraints - references

Copyright, Designs and Patents Act 1988

This Act, together with a number of Statutory Instruments that have amended and extended it, controls copyright law. It makes it an offence to copy all, or a substantial part, which can be a quite small portion, of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, sound, moving images, TV broadcasts and many other media.

Malicious Communications Act 1988

Under this Act it is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person. Additionally, under the Telecommunications Act 1984 it is a similar offence to send a telephone message, which is indecent, offensive, or threatening.

Computer Misuse Act 1990

This Act makes it an offence

- to erase or amend data or programs without authority;
- to obtain unauthorised access to a computer;
- to "eavesdrop" on a computer;
- to make unauthorised use of computer time or facilities;
- maliciously to corrupt or erase data or programs;
- to deny access to authorised users.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- display any writing, sign or other visible representation which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Trade Marks Act 1994

This Act provides protection for Registered Trade Marks, which can be any symbol (words or images) or even shapes of objects that are associated with a particular set of goods or services.

Anyone who uses a Registered Trade Mark without permission can expose themselves to litigation. This can also arise from the use of a Mark that is confusingly similar to an existing Mark.

Data Protection Act 1998

The Group has a comprehensive Data Protection Policy, of which the following statement is the summary:

Everyone has rights with regard to how their personal information is handled. During the course of our activities we will collect, store and process personal information about our staff, and we recognise the need to treat it in an appropriate and lawful manner.

The types of information that we may be required to handle include details of current, past and prospective employees, suppliers, stakeholders and others that we communicate with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 1998 (the Act) and other regulations. The Act imposes restrictions on how we may use that information.

This policy does not form part of any employee's contract of employment and it may be amended at any time. Any breach of this policy by a member of staff will be taken seriously and may result in disciplinary action.

The Group manages and maintains belief that protecting the privacy of our staff and learners and regulating their safety through data management, control, and evaluation is vital. The Group collects personal data from learners, parents, and staff and processes it in order to support teaching and learning, monitor and report on learner and teacher progress, and strengthen our pastoral provision.

We take responsibility for ensuring that any data that we collect and process is used correctly and only as is necessary, and the Group will keep parents fully informed of the how data is collected, what is collected, and how it is used. National curriculum results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of data that the Group needs. Through effective data management we can monitor a range of provisions and evaluate the wellbeing and academic progression to ensure that we are doing all that we can to support all stakeholders.

Human Rights Act 1998

This act does not set out to deal with any particular mischief or address specifically any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the context of the Group, important human rights to be aware of include:

- the right to a fair trial
- the right to respect for private and family life, home and correspondence
- freedom of thought, conscience and religion
- freedom of expression
- freedom of assembly
- prohibition of discrimination

- the right to education

These rights are not absolute. The Group, together with all users of its ICT services, is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations which arise from other relevant legislation.

Regulation of Investigatory Powers Act 2000

The Act states that it is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic (including telephone) communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.

Freedom of Information Act 2000

The Act, intended to increase openness and transparency, obliges public bodies, including Educational Institutions, to disclose a wide range of information, both proactively and in response to requests from the public. The types of information that may have to be found and released are wide-ranging, for example minutes recorded at a board meeting of the institution or documentation relating to important resolutions passed. Retrieval of such a range of information places a considerable burden on an institution subject to such an information request. In addition to setting a new standard of how such bodies disseminate information relating to internal affairs, the Act sets time limits by which the information requested must be made available, and confers clearly stated rights on the public, regarding such information retrieval. Therefore, all staff have a responsibility to know what information they hold and where and how to locate it.

Communications Act 2003

This act makes it illegal to dishonestly obtain electronic communication services, such as e-mail and the World Wide Web.

Criminal Justice and Immigration Act 2008

This act increased the penalties for publishing an obscene article. It also introduced fines for data protection contraventions when organisations 'knew or ought to have known that there was a risk that the contravention would occur, and that such a contravention would be of a kind likely to cause substantial distress or damage, but failed to take reasonable steps to prevent the contravention.'

Appendix 2

Sample Acceptable Use of Technologies Agreements

This section contains samples for different categories of users
The Group Staff & volunteers (including guests)

The Group Staff & Volunteers (including guests)

This Acceptable Use Agreement is intended to ensure that:

- Staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- The Group ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Staff are protected from potential risk in their use of ICT in their everyday work.

The Group will try to ensure that staff and volunteers have good access to ICT to enhance their work, to enhance learning opportunities for learners and will, in return, expect staff and volunteers to agree to be responsible users.

- I understand that I must use the Group's ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.
- I recognise the value of the use of ICT for enhancing learning and will ensure that learners receive opportunities to gain from the use of ICT.
- I will, where possible, educate the learners in my care in the safe use of ICT and embed e-safety in my work with learners.

For my professional and personal safety:

- I understand that the Group will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of the Group's ICT systems (e.g. personal learning devices, laptops, email, online learning space, LMS etc.) out of the Group.
- I understand that the Group's ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the Group
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using the Group's ICT systems:

T:C Partnership
Training • Education • Careers

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the Group's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the Group's website / the Group's Online Learning Space) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in accordance with the Group's policies.
- I will only communicate with learners and parents / carers using official systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.

The Group has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the Group:

- When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc.), I will follow the rules set out in this agreement, in the same way as if I was using the Group equipment. I will also follow any additional rules set by the Group about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the Group's ICT systems.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful software.
- I will ensure that my data is saved on the Group's network and where this is not possible that it is backed up, in accordance with the relevant Group policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programs or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet bandwidth and prevent other users from being able to carry out their work.
- I will not install or attempt to install programs of any type on a device, or store programs on a computer, nor will I try to alter computer settings, unless this is allowed.
- I will not disable or cause any damage to group equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others. Where personal data is transferred outside the secure Group network, it must be encrypted.
- I understand that The Group Data Protection Policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by the Group policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for the Group sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the Group:

- I understand that this Acceptable Use Agreement applies not only to my work and use of the Group ICT equipment in the Group, but also applies to my use of the Group's ICT systems and equipment out of the Group and my use of personal equipment in the Group or in situations related to my employment by the Group.
- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Group Council and / or the Group and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the Group's ICT systems (both in and out of the Group) and my own devices (in the Group and when carrying out communications related to the Group) within these guidelines.

Staff / Volunteer Name	
Signed	
Date	