Information Technology and Communications Acceptable Use Policy

Purpose

The Reaseheath Group seeks to promote and facilitate the proper and extensive use of Information Technology in the interests of learning and research. This requires responsible and legal use of the technologies and facilities made available to students and staff.

This Acceptable Use Policy is intended to provide a framework for such use of the Reaseheath Group's ICT resources.

Members of the Reaseheath Group and all other users of the group's facilities are bound by the provisions of these policies in addition to this Acceptable Use Policy. They are also bound by any other Group policies that may reference any IT services. It is the responsibility of all users of Reaseheath Group's Information Technology services to read and understand this policy.

This policy is part of the group's Information Security Management System based on ISO 27001 International Standard for Information Security. Specifically ISO 27002 Clause 8.1.3 Acceptable Use of Assets and 7.2.2 Information security awareness, education and training.

Audience

This policy is intended to be read and understood by all users accessing the Reaseheath information, IT systems, networks or software using any Group or personally owned device.

It applies to all computing, telecommunication, and networking facilities provided by any department or section of the Reaseheath Group.

Definitions

Reaseheath Group: For the purposes of the Information Security Management System, the Reaseheath Group is comprised of Reaseheath College, Reaseheath University Centre, Burrows Lane Equestrian Centre and Croft End Equestrian Centre.

Main Site: Reaseheath Campus, Nantwich CW5 6DF

Designated Authority: Vice Principal Finance and Resources, Deputies: ICT Operations Manager and ICT Systems and Infrastructure Manager.

Overview

Reaseheath Group ICT resources are provided primarily to facilitate a person's essential work as an employee or student or other role within the Reaseheath Group.

College e-mail addresses and associated Reaseheath Group e-mail systems must be used for all official Reaseheath Group business, in order to facilitate auditability and institutional record keeping. All staff and students of the Reaseheath Group must regularly read their Reaseheath Group e-mail.

Users must not use a Reaseheath Group email address for purposes other than those permitted by this clause unless special permission has been granted. In particular, users must not use or advertise their Reaseheath email address for any non-Group business or for campaigning or any party political purpose without the prior permission of the designated authority.

Use for other purposes, such as personal electronic mail or recreational use of the World Wide Web, is a privilege, which can be withdrawn, not a right.

Although not a right, limited personal use is permitted, provided it does not interfere with a member of staff's work nor adversely affect a student's studies. Personal/recreational use of the IT facilities may be subject to temporary or permanent suspension if necessary to ensure service continuity or the availability of adequate resources for research, learning and teaching, and/or administrative use.

Any such use must not, in any way, bring the Reaseheath Group into disrepute. Priority must always be granted to those needing facilities for academic work.

Commercial work for outside bodies, using centrally managed services, requires explicit permission from the Vice Principal Finance and Resources; such use, whether or not authorised, may be liable to charge.

Authorisation

In order to use the computing facilities of Reaseheath Group an individual must have an account assigned. Account creation for all members of staff is carried out via an automated process authorised by HR.

Student accounts are normally created as part of the registration process. Others must apply via the IT Services helpdesk.

Use of a Reaseheath Group account and any Reaseheath Group IT facilities constitutes acceptance of this Acceptable Use policy, which apply subject to, and in addition to, the law.

A user account grants authorisation to use the core IT facilities of the Reaseheath Group. Following account creation, a username, password and e-mail address will be allocated. Authorisation for other services may be requested by application to IT Services.

All individually allocated usernames, passwords and e-mail 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 particular personal username must not be divulged to any other person, other than to designated members of IT staff for the purposes of system support.

Attempts to access or use any username, e-mail address or certificate, which is not authorised to the user, are prohibited. No one may use, or attempt to use, IT resources allocated to another person, except when explicitly authorised by the provider of those resources.

All users must correctly identify themselves at all times. A user must not masquerade as another, withhold their identity or tamper with audit trails. A user must take all reasonable precautions to protect their resources. In particular, passwords used must adhere to current password policy and practice. Advice on

what constitutes a good password may be obtained from IT Services. This advice must be followed: failure to do so may be regarded as a breach of this policy.

Privacy

The Reaseheath Group reserves the right, consistent with the relevant legislation, to exercise control over computer resources and to use any system-generated files (such as log files and error/exception reports) along with management tools to maintain system performance and investigate system faults as well as breaches, or possible breaches, of these regulations.

The Reaseheath Group also reserves the right to inspect any items of computer equipment connected to the network. Any IT equipment connected to the Group's network will be removed if it is deemed to be breaching Reaseheath Group policy or otherwise interfering with the operation of the network.

It should be noted that IT Services staff and other administrative Staff users, who have appropriate privileges, have the ability, which is occasionally required, to access all files, including electronic mail files, stored on a computer that they manage. It is also occasionally necessary to intercept network traffic. In such circumstances, appropriately privileged staff will take all reasonable steps to ensure the privacy of service users.

Reasons for such monitoring may include the need to:

- Ensure operational effectiveness of services
- Prevent a breach of the law, this policy, or other Reaseheath Group policy
- Investigate a suspected breach of the law, this policy, or other Reaseheath Group policy
- Monitor standards
- Ensure e-safety standards are supported and provide safe internet facilities to students and staff
- To support HM Government Prevent Programme in helping prevent people from being drawn into terrorism/extremism.

Access to staff files, including electronic mail files, will not normally be given to another member of staff unless authorised by the Vice Principal Finance and Resources or his designated Deputy. In such circumstances the Head of Department or Section, or more senior line manager, will be informed, and will normally be consulted prior to action being taken. Such access will normally only be granted where it is required for the purpose of an investigation or monitoring in line with the Reaseheath Group's policies or procedures or where a breach of the law or a serious breach of this policy is suspected, or when a documented and lawful request from a law enforcement agency such as the police or security services has been received.

The Reaseheath Group sees student privacy as desirable but not as an absolute right, hence students should not expect to hold or pass information, which they would not wish to be seen by members of staff responsible for their academic work. In addition to when a breach of the law or of this policy is suspected, or when a documented and lawful request from a law enforcement agency such as the police or security services has been received, systems staff are also authorised to release the contents of a student's files, including electronic mail files, when required to by any member of staff who has a direct academic work-based reason for requiring such access.

All files including electronic mail files and image files that are stored on the Group's IT systems are considered the property of the Reaseheath Group. Any files, documents, applications or images produced using the Group's IT Services equipment are the property of the Reaseheath Group and as such, the Reaseheath Group reserves the intellectual Copyright.

After a student or member of staff leaves the Reaseheath Group, files that are left behind on any computer system owned by the Reaseheath Group, including servers, and including electronic mail files, will be considered the property of the Reaseheath Group. When leaving the Reaseheath Group, staff should arrange to transfer to colleagues any e-mail or other computer-based information held under their personal account, as this will be closed on their departure.

E-safety

The Reaseheath Group is dedicated to ensuring that all students and staff can use the Reaseheath Group's systems safely and be protected against cyberbullying, web fraud, access to unsuitable images/documents, grooming and the possibility of being drawn into terrorism or extremism (Prevent).

Therefore, the Reaseheath Group actively carries out website, application, Malware, Virus blocking, and countermeasures using particular categories, websites and keywords.

The categories and keywords authorised to be blocked are regularly reviewed by IT Services.

Alerts can be generated upon sustained attempts to access sites/categories, monthly reports are produced, and any suspicious activity checked and monitored by IT Services and reported to Senior Management as required.

Behaviour

No person shall jeopardise the integrity, performance or reliability of computer equipment, software, data and other stored information. The integrity of the Reaseheath Group's computer systems is put at risk if users do not take adequate precautions against malicious software, such as computer virus programs. All users of Reaseheath Group IT services must ensure that any computer, for which they have responsibility and which is attached to the Reaseheath Group network, is adequately protected against viruses, through the use of up to date anti-virus software (any exceptions to this must be approved explicitly by IT Services), and has the latest tested security patches installed. Reasonable care should also be taken to ensure that resource use does not result in a denial of service to others.

Conventional norms of behaviour apply to IT-based media, just as they would apply to more traditional media. The Reaseheath Group, as expressed in its Equality, Diversity and Inclusion Policy, is committed to achieving an educational and working environment that provides equality of opportunity, and freedom from discrimination on the grounds of race, religion, sex, class, sexual orientation, age, disability or special need.

Distributing material, which is offensive, obscene or abusive, may be illegal and may contravene Reaseheath Group codes on harassment. Users of Reaseheath Group computer systems must make themselves familiar with, and comply with, the Reaseheath Group code of conduct on harassment and bullying.

Use of the Reaseheath Group IT facilities must not bring the institution into disrepute.

Users must not tamper with, or cause damage to, the Reaseheath Group IT facilities, nor to any of the accommodation or services associated with them.

Users must adhere to the terms and conditions of all licence agreements relating to IT facilities and information that they use including software, equipment, services, documentation and other goods.

Users must not infringe intellectual property rights or copyright works in any form including software, documents, images, or audio or video recordings.

Users must not install any software or other copyright material onto any shared IT facility, or in such a way that other users, without permission from the copyright owner and the designated authority, may access it.

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 should apply to electronically held information as to that held on traditional media such as paper.

Users must not act in any way that puts the security of the IT facilities at risk. In particular, usernames and passwords must be kept safe and secure and only used by those authorised to do so. Passwords must never be divulged to others by any means.

Users must never use login details other than their own to access the IT facilities nor allow others to use the IT facilities they are connected to without logging out and disconnecting first. Users must not store IT account credentials in such a way that any other user of the device could use their access rights.

Users with system administration accounts must use a different password to their user account. The Reaseheath Group reserves the right, without prejudice, to issue a warning to, or take other appropriate action (including disciplinary action) against, users who are responsible for security breaches.

Users must not, in their use of IT facilities, exceed the terms of the permissions associated with their IT account. In particular, they must not connect to, or attempt to connect to, any IT facility without the appropriate permission. This is known as hacking and is a criminal offence under the Computer Misuse Act 1990, as amended.

Users must log out from their account and make their computer and network connection secure against unauthorised use whenever they are not actively using the machine.

Users must not allow anyone else to use a network connection provided for their personal use or provide any services to others via remote access.

Users may be liable for the cost of remedying any damage they cause or to which they contribute.

Users of networks and remote IT facilities shall obey any rules (such as the JANET Acceptable Use Policy available at https://community.jisc.ac.uk/library/acceptable-use-policy) that may be published from time to time for their use.

Reaseheath Group business must be conducted using Reaseheath Group email accounts rather than personal accounts.

For specific services, the Reaseheath Group may provide more detailed guidelines, in addition to the information provided in this Acceptable Use Policy.

Users should not carry out activities utilising the IT facilities that will interfere with the work of other users nor should they attempt to prevent the legitimate use of the IT facilities by others.

Users must not attempt to conceal or falsify the authorship of any electronic communication.

Users must not send unsolicited electronic communications to multiple recipients except where it is a communication authorised by the Reaseheath Group. Specifically, users must not send spam or chain letters. If in doubt, advice must be sought from the designated authority.

The Reaseheath Group has a statutory duty, under the Counter Terrorism and Security Act 2015, termed 'PREVENT'. The purpose of this duty is to aid the process of preventing people being drawn into terrorism.

You must not create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening, discriminatory or extremist. The Reaseheath Group reserves the right to block or monitor access to such material. The interpretation will normally be the responsibility of the Safeguarding lead, but will be applied in the first instance by the IT Services team. Any such material that is introduced to the IT facilities will be removed forthwith. Where access to such material is deemed necessary, prior permission must be sought from the designated authority and safeguarding lead.

Use of the TOR browser (The Onion Router) and other similar forms of anonymous internet activity from within the Reaseheath Group network are restricted for reasons of IT Security. Where users have a genuine requirement to use TOR for academic or professional purposes, approval will be required by the designated authority.

Users of services external to the Reaseheath Group 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 Reaseheath Group credentials to gain unauthorised access to the facilities of any other organisation is similarly prohibited.

Equipment

Users are responsible for ensuring that they are sufficiently familiar with the operation of any equipment they use in order to access the IT facilities to make their use of it safe and effective and to avoid interference with the use of it by others.

Non-portable Reaseheath Group equipment may not be moved or removed without the prior agreement of the designated authority.

No equipment may be connected in any way into any network or other IT facility of the Reaseheath Group without the prior agreement of the designated authority.

Users must make any changes specified by Reaseheath IT Services in order to safeguard the Reaseheath Group's IT facilities and users thereof. If the changes are not carried out, Reaseheath Group reserves the right to disable network connection until the device is secured or the vulnerability has been removed.

Disposal of computing equipment must be done safely and securely, in accordance with the Reaseheath Group's policies and contractual obligations, including the Disposal of IT Equipment Policy. All data and software must be securely removed and the requirements of the WEEE Directive must be met.

Definitions of Acceptable & Unacceptable Usage

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

The retention or propagation of material that is offensive, obscene or indecent, except in the course of recognised research or teaching that is permitted under UK and international law; propagation will normally be considered to be a much more serious offence;

- intellectual property rights infringement, including copyright, trademark, patent, design and moral rights;
- causing annoyance, inconvenience or needless anxiety to others, as specified in the JANET Acceptable Use Policy https://community.jisc.ac.uk/library/acceptable-use-policy;
- defamation;
- unsolicited advertising, often referred to as "spamming";
- sending e-mails 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;
- actions or inactions which intentionally, or unintentionally, aid 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 Reaseheath Group network for unauthenticated access;
- Unauthorised resale of Reaseheath Group or JANET services or information.
- Connecting networking devices to the network.

These restrictions should be taken to mean, for example, that the following activities will normally be considered to be a breach of this policy (potential exceptions should be discussed with IT Services):

- The downloading, distribution, 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;
- Connecting an unauthorised device to the Reaseheath Group network, i.e. one that has not been configured to comply with this policy and any other relevant regulations and guidelines relating to security, I.T. 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 router/Access points, to which you are not authorised;
- Adding routers, switches, wireless access points or any equipment that is capable of distributing network services;
- Non-academic activities which generate heavy network traffic, especially those which interfere with others' legitimate use of I.T. services or which incur financial costs;
- Excessive use of resources such as file areas, leading to a denial of service to others, especially when compounded by not responding to requests for action;
- Frivolous use of Reaseheath Group owned Computer laboratories, especially where such activities interfere with others' legitimate use of I.T. services;
- The deliberate viewing and/or printing of pornographic images;
- The passing on of electronic chain mail;
- The use of Reaseheath Group business mailing lists for non-academic purposes;
- The use of CDs, DVDs, and other storage devices for the purpose of copying unlicensed copyright software, music, etc.;
- The copying of other people's web site material without the express permission of the copyright holder;
- The use of peer-to-peer and related applications within the Reaseheath Group. These include, but are not limited to, Ares, BitTorrent, Direct Connect, Morpheus, KaZaA;
- Plagiarism i.e. the intentional use of other people's material without attribution.

Other uses may be unacceptable in certain circumstances. In particular, users of the Hostel Internet Service should take account any particular conditions of use applying to that service. It should be noted that Hostel Service users should not provide any services to others via remote access. The installed machine on each network socket must be a workstation only and not provide any server-based services, including, but not limited to, Web, FTP, IRC, Streaming Media server, peer-to-peer facilities, or e-mail services.

It should be noted that individuals may be held responsible for the retention of attachment material that they have received, via e-mail that they have never opened, via e-mail that they have read. Similarly, opening an attachment, received via unsolicited e-mail, especially if clearly unrelated to work or study, which leads to widespread virus infection, may result in disciplinary action being taken.

Acceptable uses may include:

- Personal e-mail and recreational use of Internet services, as long as these are in keeping with the framework defined in this policy document and do not interfere with one's duties, studies or the work of others;
- Advertising via electronic notice boards, intended for this purpose, or via other Reaseheath Group approved mechanisms.

Legal Constraints

Any software and / or hard copy of data or information which is not generated by the user personally and which may become available through the use of Reaseheath Group computing or communications resources shall not be copied or used without permission of the Reaseheath Group or the copyright owner. In particular, it is up to the user to check the terms and conditions of any licence for the use of the software or information and to abide by them. Software and/or information provided by the Reaseheath Group may only be used as part of the user's duties as an employee or student of the Reaseheath Group or for educational purposes.

The user must abide by all the licensing agreements for software entered into by the Reaseheath Group with other parties, noting that the right to use any such software outside the Reaseheath Group will cease when an individual leaves the institution.

When an individual leaves the Reaseheath Group, they are not permitted to remove any information from Reaseheath Group equipment that is the property of the Reaseheath Group. Any software on a privately owned computer that has been licensed under a Reaseheath Group agreement must be removed from it, as well as any Reaseheath Group-owned data, such as documents and spreadsheets.

When a computer ceases to be owned by the Reaseheath Group, all data and software must be removed from it, in accordance with the Reaseheath Group's policies and contractual obligations, including the Computer Equipment Disposal Policy.

In the case of private work and other personal use of computing facilities, the Reaseheath Group will not accept any liability for loss, damage, injury or expense that may result.

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

This section contains a list of laws and policies that may apply to use of IT facilities. Note that this list may not be exhaustive and will be subject to amendments and any superseding legislation that may be enacted.

The legislation can be viewed via www.legislation.gov.uk. Those who use the facilities from outside the UK may be bound by the laws of the UK and / or any other applicable local laws.

- General Data Protection Regulation
- Obscene Publications Act 1959 & 1964
- Protection of Children Act 1978
- Police and Criminal Evidence Act 1984
- 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 2018
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Communications Act 2003
- Counter Terrorism and Security Act 2015
- Terrorism Act 2006 Police and Justice Act 2006
- Digital Economy Act 2017
- Equality Act 2010
- Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011

Infringement

Any infringement of these regulations may be subject to penalties under civil or criminal law and such law may be invoked by the Reaseheath Group. In addition, the use of computer software and other material may also be subject to the terms of licence agreements into which the Group has entered. Use of the Group's systems may be logged to permit the detection and investigation of infringement of policies and / or licence agreements.

In cases of infringement or possible infringement of these regulations, the Reaseheath Group reserves the right to suspend an offending user's connection (temporarily or permanently) and / or to withdraw access to facilities. Any withdrawal of service may be notified to the user's Head of Department.

Any infringement of these regulations may constitute a disciplinary offence under the applicable procedure for members of staff or students. Reaseheath Group may commence disciplinary proceedings against a member of staff or a student following a breach or alleged breach of the regulations. Minor infringements of these regulations may be dealt with informally without recourse to the formal disciplinary procedure. Breaches of these regulations that have a serious or potentially serious adverse consequence for the Group's operation, business / academic activities or reputation, or for the security / integrity of the IT systems may constitute gross misconduct and render the offender liable to dismissal.

The Reaseheath Group reserves its right to take legal action against individuals who cause it to be involved in legal proceedings as a result of their violation of licensing agreements and/or other contraventions of this policy.

Policy Supervision and Advice

The responsibility for the supervision of this Acceptable Use Policy is delegated to IT Services. A senior member of IT Services, normally the Systems and Infrastructure Manager, will be designated as the person responsible for the day-to-day management of the policy's enforcement. They will liaise with the Vice

Principal Finance and Resources, Vice Principal Curriculum and Quality, the Reaseheath Group Librarian, the Security Manager, the Director of People and Culture, the Registrar, and Heads of Department and Sections, as required. Procedural guidelines will be published from time to time as a separate document.

Any suspected breach of this policy should be reported to a member of IT Services in accordance with the Incident Response Procedure. The responsible senior member will then take the appropriate action within the Reaseheath Group's disciplinary framework, in conjunction with other relevant branches of the Reaseheath Group. IT Services staff will also take action when infringements are detected in the course of their normal duties. Actions will include, where relevant, immediate removal from online information systems of material that is believed to infringe the law.

The Reaseheath Group reserves the right to audit and / or suspend without notice any account pending any enquiry. Where necessary, this will include the interception of electronically mediated communications.

This policy is not exhaustive and inevitably new social and technical developments will lead to further uses, which are not fully covered. In the first instance, students should address questions concerning what is acceptable to their supervisor; staff should initially contact their Head of Department. Where there is any doubt the matter should be raised with IT Services, whose staff will ensure that all such questions are dealt with at the appropriate level within the Reaseheath Group.

Disclaimer

The Reaseheath Group makes no representations about the suitability of this service for any purpose. All warranties, terms and conditions with regard to this service, including all warranties, terms and conditions, implied by statute, or otherwise, of satisfactory quality, fitness for a particular purpose, and non-infringement are excluded to the fullest extent permitted by law.

The Reaseheath Group shall not in any event be liable for any damages, costs or losses (including without limitation direct, indirect, consequential or otherwise) arising out of, or in any way connected with, the use of the service, or with any delayed access to, or inability to use the service and whether arising in tort, contract, negligence, under statute or otherwise.

Version	November 2019
Effective Date	November 2019
Review date	April 2020 reviewed August 2021 reviewed Next review November 2022
Lead Director	Vice Principal Finance and Resources
Approved by	Executive 12.11.19 Finance and General Purposes Committee Executive 16.08.21
Published on	Staff intranet, Student intranet, College website
Date of Equality Analysis	N/A
Changes on Review	Update to staff titles: April 2020 Update to group definition: August 2021