fircroftcollege

IT Security Policy

POLICY / DOCUMENT PURPOSE STATEMENT

The purpose of this policy is to present the guidelines and standards that users must adhere to when accessing the College IT infrastructure, preserving the security and availability of the College IT infrastructure and all data held within. This policy aims to facilitate users so they do not unintentionally place the College or themselves at risk when using and accessing IT systems.

APPLICATION

The policy applies to all individuals accessing the college IT systems and data held within.

INTERPRETATION

Further guidance on the use or interpretation of this policy may be obtained from the IT department.

LINKS WITH OTHER POLICIES / DOCUMENTS

Emergency Planning Procedure, Fircroft IT User Agreement, Fircroft College BYOD Policy, Fircroft Email, Internet & Wi-Fi Policy, IT Call Logging and Escalation Policy Staff, Disciplinary Policy & Procedure, Code of Professional Standards.

Version number	1
Owner / Department	Andy Gazey/IT
Date of Implementation	06/12/2021
Review date	30/01/2024
Ratified / Authorised by	08/02/2023
Equality Impact completed	06/12/2021

IT Security Policy

Table of Contents

Introduction Page 4
Confidentiality Page 4
Data Management Page 4
Network Security Page 5
User Authentication and Audit Logging Page 5
Encryption Page 6
IT Security Training Page 6
Integrity Page 7
User Access and Audit Logging Page 7
Vulnerability Management Page 7
Change Management Page 8
Availability Page 8
Software Licensing and Maintenance Page 8
Disaster Recovery and Backup Strategy Page 8
Incident Management Page 9
Security Operations Page 9
Physical Computer Storage Environmental Provisions Page 9
General standards of IT Usage Page 9
Standards of Computer usage Page 10
Monitoring Page 11

1. Introduction

1.1. This policy is for all users of the Colleges' IT environment and aims to maintain and continually improve the security of the college IT systems and all data held within, protecting the IT facilities, data, and information stored and all users of the College IT environment.

1.2. This policy will present the standards and guidelines which aim to preserve and improve the security, confidentiality, and availability of the College IT systems and all data held within.

1.3. All information stored on College IT systems will be stored in a secure manner and safeguards are in place to prevent unauthorised access.

1.4. It is therefore essential that users read and agree to be bound by these guidelines and make themselves aware of the potential legal liabilities involved in using and accessing the College IT environment.

1.5. This policy will be reviewed and updated to reflect changes in technology and new developments within the Colleges IT environment.

2. Confidentiality

Safeguarding the confidentiality of information through the protection of information from authorised disclosure with access only by entitlement.

2.1. Data Management

2.1.1. Fircroft College is obligated to respect the rights of individuals and to protect confidential data.

2.1.2. All college digital records should be classified according to the Data Protection Policy (Appendix A).

2.1.3. When data is classified as confidential or sensitive, appropriate access and security controls are applied in transmission and storage. Confidential or sensitive data is not to be transmitted without adequate precautions being taken to ensure that only the intended recipient can access the data.

2.1.4. All college information is to be treated as sensitive if not otherwise indicated.

2.1.5. Where the college engages in the use of cloud or external hosting services, which will host college data, the proposed solutions must be evaluated by the Colleges' risk assessment framework. All external services must have forced Multi-Factor authentication enabled where available.

2.1.6. Before the college network is accessed by any third parties (suppliers, contractors, consultants) for support and maintenance provided to the college, the third-party organisation will complete the College's General Privacy Notice.

2.2. Network Security

2.2.1. The college maintains a perimeter firewall. All externally facing services must be registered, this register is used to configure the firewall based on the services they offer. This eliminates low-level vulnerability probing attacks from the internet while allowing access to registered services.

2.2.2. In addition to the perimeter firewall, some network ranges are protected by access lists or additional firewalls.

2.2.3. Perimeter traffic is logged and appropriately monitored for security purposes through the JISC-controlled Janet network.

2.2.4. Laptops and desktops that connect to the college's internal network must have:

2.2.4.1. Anti-virus installed and up-to-date
2.2.4.2. Operating System patched with latest security updates
2.2.4.3. Personal firewall active
2.2.4.4. User authentication

2.3. User Authentication and Audit Logging

2.3.1. Authentication is required for each connection to the College network.

2.3.2. Where available, multi-factor user authentication will be forced for IT systems that process sensitive data.

2.3.3. Users must follow best practices to prevent misuse, loss, or unauthorised access to systems:

2.3.3.1. Keep passwords confidential
2.3.3.2. Passwords used must be unique, complex, and difficult to guess, using a mixture of characters, numbers, and special characters. Password advice can be found on the colleges IT SharePoint site.
2.3.3.3. Passwords must be changed regularly.
2.3.3.4. Never write down passwords or store passwords insecurely.
2.3.3.5. Never disclose passwords, or send passwords via email, text, or post.
2.3.3.6. External passwords must be unique and not a duplicate of your Fircroft passwords for any external sites and services.

2.3.4.7 Do not leave your computer unattended without locking your computer *(by Using Windows key + L)* or logging off the system. Never allow any other users to use your login accounts for any reason.

2.4. Encryption

2.4.1. All college-owned laptops must have their internal hard drive encrypted.

2.4.2. All college-provided mobile devices that host college data must be protected by encryption and layered authentication where appropriate. This layered authentication aims to protect devices from evolving forms of elicit fraudulent access i.e. in person or live video as voice notes or even full non-live video calls can now be replicated and used to breach encryption processes.

2.4.3. Where data is being stored by the college on a laptop or portable device, they may leave college premises, then this data should be encrypted in accordance with the college encryption guidelines and ensure compliance with the college's data protection policy.

2.4.4 Data should only be stored on College-owned and approved devices and sensitive data should never be stored on external media such as External Hard Drives for USB Flash devices.

2.4.5. Where sensitive information is transmitted through a public network to an external third party, the information must be encrypted first and sent via secure channels (preferably through One Drive secure sharing).

2.4.6. WIFI networks advertised for staff business use must be encrypted using WPA2 or better.

2.5. IT Security Training

2.5.1. IT security awareness is delivered through multiple methods with the aim of raising user awareness and highlighting end-user responsibility.

2.5.2. Scheduled targeted security awareness training sessions are available on demand in conjunction with Data Protection training.

2.5.3. Comprehensive online training sessions are available via the IT SharePoint site.

2.5.4. On staff induction new hires are briefed on the data protection policy and IT procedures.

2.5.5. New learners are briefed on the data protection policy and IT procedures in their course induction.

3. Integrity

Safeguarding the integrity of information I.e. the accuracy and completeness of information by protecting against unauthorised modification

3.1. User Access and Audit Logging

3.1.1. Access to information is granted on a needs-only basis, staff are granted specific access to allow them to carry out their job functions.

3.1.2. Access to amend information and/or access to systems which process and record this information is restricted to authorised personnel.

3.1.3. All individuals have a unique user name for their personal and sole use so that activities can be traced to the responsible person, and any access revoked where needed.

3.1.4. All access to high-criticality services is to be logged and appropriately monitored to identify potential misuse of its systems or information. Logs must be retained and access granted according to the appropriate legislation.

3.1.5. Security event logs, operational audit logs, error logs, transaction and processing logs are monitored on critical systems and retained to record events for troubleshooting, providing forensics during security incidents and to identify potential misuse of systems or information.

3.1.6. An appropriate audit trail including database logs of the creation, amendment and deletion of college data and/or systems is maintained by IT services. This is particularly important in the relation to the following:

3.1.6.1. Data including details on staff, students and suppliers

3.1.6.2 . Data including inward fee payments, outward supplier payments, payroll transactions and other financial data.

3.1.6.3. Any other Fircroft College owned data

3.2. Vulnerability Management

Anyone connecting equipment to the network is responsible for ensuring that the equipment is configured correctly, that the operating systems and software applications are up-to-date as regards patch management etc. and that the equipment has adequate protection against viruses and other malware. If there is any suspicion that the equipment may be infected or compromised it should not be connected. This should then be reported to the college's IT team.

3.2.1. Each IT service has a defined service owner. Servers supporting this service must be protected before joining the college network and should be locked down before becoming a production service. This is the IT team and the college's third-party IT provider's responsibility

.

3.2.2. College infrastructure (servers, desktops, operating systems, databases & applications) must follow a regular patch schedule to ensure IT assets remain protected from security vulnerabilities and remain within mainstream support.

3.2.3. Antivirus is a compulsory pre-requisite for any computer joining the college network. Anti-virus is controlled centrally by the college's IT team and third-party IT provider.

3.2.4. The college's Head of Business Infrastructure and IT Network Co-ordinator have the authority to remove from the network any equipment for which no owner can be identified.

3.2.5. The college's Head of Business Infrastructure and IT Network Co-ordinator has the authority to remove from the network any equipment which is interfering with the network service or is deemed likely to compromise the security of the network. While every effort will be made to contact the owner of the equipment in advance, maintaining the service must take precedence.

3.3. Change Management

3.3.1. System changes should aim to be completed outside of core delivery hours with at least 10 working days' notice given for any none critical changes.

3.3.2. All system changes must be logged and recorded in line with best practice guidance.

4. Availability

Maintaining the availability of the college's information and IT systems for business process usage as required.

4.1. Software Licensing and Maintenance

4.1.1. The college IT team and third-party IT provider must ensure that all software licenses are up-to-date and that maintenance support is available for both the hardware and software associated with these services.

4.1.2. Desktop software licensing for standard software is managed centrally through site licensing for staff. Licensing for non-standard software is the user's responsibility.

4.1.3. Illegal and unlicensed software must not be installed on college-owned computers.

4.2. Disaster Recovery and Backup Strategy

4.2.1. It is the responsibility of the business owner of each service to ensure that an adequate business continuity plan is in place in the event that the service is affected by the non-availability of the relevant servers, network, or other elements of the IT infrastructure.

4.2.2. IT services maintain disaster recovery plans for all college centrally managed infrastructure and critical services.

4.2.3. Disaster recovery plans and processes are tested regularly.

4.2.4. The IT team and third-party IT provider manage data and system backups for critical systems.

4.2.5. Recovery from backup is tested bi-annually.

4.3. Incident Management

4.3.1. Formal incident management procedures are in place for any IT security incidence and procedures relating to personal data breaches.

4.4. Security Operations

4.4.1. The college IT team and third-party IT provider manage multiple security tools with the aim of protecting the IT assets and services of the college against unauthorised access, intrusion and disruption. Processes are in place to support these tools and ensure proactive management of IT vulnerabilities and reported incidents.

4.5. Physical Computer Storage Environmental Provisions

4.5.1. Any server hosting production services for the college must be housed in a suitable environment with regard to security, electrical power, air conditioning etc.

4.5.2. All hardware used for the storage of college data is to be purged of data and securely destroyed once it is no longer to be used. Please see the college's data retention policy for guidance of information retention.

4.5.3. When storage devices reach the end of their useful life, they are to be purged of college data and securely destroyed.

This security policy is intended to ensure an effective IT infrastructure for the benefit of all users. Where necessary, support will be provided by the IT team to assist users in complying with this policy.

5. General standards of IT Usage

The following standards must be adhered to and followed at all times when using and accessing College IT facilities. Further help, advice, and clarification are available by contacting IT Support (ITSupport@fircroft.ac.uk).

5.1. The use of College IT systems is primarily for work and/or study-related purposes and all users must comply with all relevant parts of this policy at all times when accessing and using the College IT environment.

5.2. Users of College IT facilities must comply with the law and Government guidelines at all times.

5.3. No attempt should be made to circumvent the College security measures and procedures in place.

5.4. Data must be protected against unwanted or unauthorised access, maintaining appropriate confidentiality.

5.5. Users must never use IT systems for the creation, storage, downloading, displaying, or sharing of any material in breach of the UK Government Prevent strategy.

5.6. Users must never use IT systems to harass, intimidate, impersonate or abuse others.

5.7. Users must never use IT systems for the creation, storage, downloading, displaying or sharing of any material of an obscene, offensive, defamatory or indecent nature.

5.8. The College IT systems must not be used to commit any form of fraud, piracy, or unauthorised use of data.

5.9. The use of any hacking techniques is strictly prohibited throughout the College IT environment.

5.10. Users must never make any attempt to damage or destroy another user's data. Another user's data must only be modified with authorisation from the data holder.

5.11. Any security incident, suspected security incident, or general security concerns must be reported to the College IT helpdesk (itsupport@fircroft.ac.uk) immediately or as soon as reasonably possible. If a suspected security incident takes place outside of normal college hours, the duty manager must be informed.

6. Standards of Computer usage

The following standards and guidelines must be adhered to and followed at all times when using and accessing College IT facilities. Further help, advice and clarification is available by contacting IT Support (ITSupport@fircroft.ac.uk).

6.1. All computer equipment must be locked when not in use, even when you are away from your device for a short period of time. *To do this, press the Windows key and the letter L*. Please ask IT support (itsupport@fircroft.ac.uk) if you are unsure how to do this. All user equipment should be shut down at the end of the day.

6.2. When using shared devices, you should shut down or log out of your active session from the device when finished.

6.3. Be aware of where you store information, for example, personal information should not be stored on general staff drives which all staff has access.

6.4. Software and Apps should not be downloaded to College IT equipment without permission from the College IT department.

6.5. All data should be stored in your college OneDrive account and relevant SharePoint sites where possible. Data should not be held on insecure devices, such as USB devices, due to their insecurities (e.g. being lost, left unattended, corrupted).

6.6. All necessary precautions should be made to prevent the loss and theft of College equipment. If a college device is lost/stolen, you must inform IT Support immediately so actions can be taken to force logouts from any open sessions to secure College data.

6.7. When transferring data, for example through emails or OneDrive file sharing, make sure the recipient address is correct. The college recommends using OneDrive to share confidential/personal information as access can be revoked at any time. OneDrive training is available on the IT Teams SharePoint site or by contacting IT Support.

6.8. Whilst the College has email filtering deployed, no system is 100% efficient at filtering all Phishing/SPAM emails, etc. You should always check for suspicious emails and verify the sender (by checking the sender's actual email address). All suspicious emails should be reported to IT (itsupport@fircroft.ac.uk) so action can be taken. It is for the user to be aware of such threats and what action should be taken.

6.9. Users must not open or reply to emails or attachments which are unmistakably from untrusted senders. Any such email should be deleted without opening and reported to IT Support for investigation and blocking.

6.10. Users must not knowingly transmit data that could compromise security, for example, an email attachment infected with a virus.

6.11. If College email accounts are accessible on personal devices (e.g. mobile phones), security methods should be in place on such devices (e.g. PIN codes, biometrics) to protect College data.

7. Monitoring

IT usage is monitored and recorded to ensure the security and availability of IT systems at all times, to protect the Colleges' reputation, and to protect the users of all college IT Systems. Activity is also monitored to fulfil the Colleges responsibilities with regard to UK law, the Government prevent agenda, and the JaNet code of conduct.

7.1. The College reserves the right to monitor internet usage in the interests of detecting or investigating improper usage of the facility in the interests of any authorised investigation, both disciplinary and legal, and also for monitoring for security reasons.

7.2. The College reserves the right to monitor, access, and investigate user data on College IT systems, including but not limited to user's data, email messaging and Teams communication methods in the interests of any authorised investigation, both disciplinary and legal.

7.3. Any suspicious, damaging or illegal activities, data may be made available to third parties, for example, An investigating officer, the College Safeguarding Officer, the College Data Protection Officer or the Police.

Appendix 1

Data Protection Issues

Personal data is subject to the Data Protection Act 2018. Under the terms of the Act, personal data includes any information about a living identifiable individual, including their name, address, phone number, e-mail address and any other information about the individual. If you include such information in an e-mail, you are deemed to be processing personal data and must abide by the law. In particular, you must not collect such information without the individual knowing you propose to do this; you may not disclose or amend such information except in accordance with the purpose for which the information was collected; and you must ensure the information is accurate and up to date. In addition, the individual has the right to inspect what is held about him or her on the e-mail system, or held in separate archives of e-mails. The individual can demand correction of inaccurate information, can request blocking or erasure of damaging information, and can sue for damage caused by inaccurate information.

The law also imposes rules on the storage of personal data. Such data should only be kept for as long as it is needed for the purpose for which it was collected. If you maintain your own stores of emails, you should ensure that such stores are not maintained for longer than is necessary for the purpose for which it was collected. E-mails should be held in such a way that they can be easily identified, reviewed and, when necessary, destroyed.

Finally, the law imposes strict rules on the transfer of personal data outside the European Economic Area (EEA). Transfer is not just the deliberate sending of information outside the EEA, but also allowing third parties from outside the EEA access to the personal data held in the UK.

Therefore, you should not:

- Use e-mails for any purpose that is not permitted under the College’s notification under the Data Protection Act;

- Use a false identity in e-mails you send out;

- Exploit mail servers or other systems to facilitate the widespread distribution of unsolicited and unwanted e-mails;

- Use e-mails for communicating confidential or sensitive matters relating to individuals;

- Obtain, handle or disclose personal information without ensuring you are complying with the law or with the College’s notification to the Data Protection Commissioner;

- Allow third parties to read personal information in e-mails or attachments by leaving your screen in view of such third parties;

- Create or forward advertisements, chain letters or unsolicited e-mails;

- Read other peoples’ e-mails sent to someone else without their express permission;

- Pass on your password or ID to any third party;

- Invade someone’s privacy by any means using e-mail;

- Send e-mails containing personal information outside the EEA, or allow third parties outside the EEA to read your e-mails containing such information without checking with the College’s Data Controller.

You should:

- Be cautious about putting personal information in the body of the text, especially if it is of a sensitive or confidential nature;

- Comply with a request from the Data Controller, your manager or a member of the Senior Leadership Team to inspect your e-mail archives and/or to print out items relevant to a particular individual if that individual demands a copy of his/her file. This will only be requested when required under the Act, or where there is good reason to believe that violations of the law or of College policies have taken place, or for some other compelling or time critical reasons;

- Agree to pass to the College all of your e-mail records if you leave the employment of the College;

Note that the recipients of your e-mails, the originators of e-mails you receive and the content of all emails sent or received may be the subject of scrutiny within current legislative provision.

Janet Acceptable Use Policy

Title:	Acceptable Use Policy
Reference:	MF-POL-006
Issue:	13
Document owner:	John Chapman, Head of Janet policy and strategy
Authorised by:	Jeremy Sharp, Janet CTO
Date:	3 March 2022 (Effective from 1 April 2022)
Last reviewed:	3 March 2022

Document control

1. Superseded documents: MF-POL-006 issue 12, dated May 2016

2. Changes made: Harmonising of definitions across policies

3. Changes forecast: None

Background

1. The Janet Network ("Janet") is the communications network operated by Jisc Services Ltd (Jisc) to serve UK education, research and other public sector purposes. Its primary purpose is to enable organisations in these communities to fulfil their missions of providing education, research, of supporting innovation, and of civic engagement more widely.

2. This Acceptable Use Policy applies to two broad categories of organisation: those connecting directly to Janet in their own right ("Connected Organisation"); and those connecting indirectly, as a partner to the directly-connected organisation and with the connection made through the latter organisation's own connection(s) to Janet ("Partner Organisation"). It also covers the granting of access to Janet to guests visiting an organisation with a Janet connection. In conjunction with MF-POL-007 the Janet Security Policy, it is an integral part of GEN-DOC-009 the Terms for Provision of the Janet Service (Janet Terms)[1].

3. The Acceptable Use Policy does not determine the eligibility of any particular organisation or individual to have a connection to and use Janet

services. This eligibility is determined by MF-POL-053 the Janet Network Connection Policy. The Acceptable Use Policy merely defines acceptable and unacceptable use of Janet by those who have been provided with access to Janet services under the terms of the Janet Network Connection Policy.

4. Copies of the Janet Terms, the Janet Network Connection Policy and the Janet Security Policy may be found at ji.sc/policies.

The Policy

Acceptable Use

5. Connected Organisations and their Partner Organisations may use Janet for the purpose of communicating with other Connected Organisations, and with organisations, individuals and services attached to networks which are reachable via Janet. All use of Janet is subject to the Janet Terms.

6. Subject to clauses 8 to 16 below, Janet may be used by a Connected Organisation for any lawful activity in furtherance of the missions of the Connected Organisation. Use by the Connected Organisation may be in pursuance of activities for commercial gain as well as for not-for-profit activities. (See Note 1)

7. It is the responsibility of the Connected Organisation to ensure that its users (and their Partner Organisations) use Janet services in accordance with the Acceptable Use Policy, and with current legislation. (See Note 2)

Unacceptable Use

8. Janet may not be used by a Connected Organisation, Partner Organisation or their users for any activity that may reasonably be regarded as unlawful or potentially so. This includes, but is not limited to, any of the following activities. (See Note 3)

9. Creation or transmission, or causing the transmission, of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material. (See Note 4)

10. Creation or transmission of material with the intent to cause annoyance, inconvenience or needless anxiety.

11. Creation or transmission of material with the intent to defraud.

12. Creation or transmission of defamatory material.

13. Creation or transmission of material such that this infringes the copyright of another person.

14. Creation or transmission of unsolicited bulk or marketing material to users of networked facilities or services, save where that material is embedded within, or is otherwise part of, a service to which the user or their User Organisation has chosen to subscribe.

15. Deliberate unauthorised access to networked facilities or services.
(See Note 5 and Note 6)

16. Deliberate or reckless activities having, with reasonable likelihood, any of the following characteristics:

16.1. wasting staff effort or Jisc resources, including time on end systems on another Connected Organisation's network, and the effort of staff involved in the support of those systems;

16.2. corrupting or destroying other users' data;

16.3. violating the privacy of other users;

16.4. disrupting the work of other users;

16.5. denying service to other users (for example, by overloading of access links or switching equipment, of Janet services, or of services or end systems on another Connected Organisation's network);

16.6. continuing to use an item of software or hardware after the Janet Network Operations Centre or its authorised representative has requested that use cease because it is causing disruption to the correct functioning of Janet;

16.7. other misuse of Janet, such as the introduction of viruses, malware, ransomware or other harmful software via Janet to resources on Janet, or on another Connected Organisation's network.

Access to Other Networks via Janet

17. Where Janet is being used to access another network, any deliberate or persistent breach of the acceptable use policy of that network will be regarded as unacceptable use of Janet. Any activity as described in clause 16 above, and where applied either to a user of that network, or to an end system attached to it, will also be regarded as unacceptable use of Janet.

18. Any deliberate or persistent breach of industry good practice (as represented by the current standards of the London Internet Exchange) that is likely to damage the reputation of Jisc will also be regarded prima facie as unacceptable use of Janet.

Compliance

19. It is the responsibility of the Connected Organisation to take reasonable steps to ensure its users, Partner Organisations and their users comply with the conditions set out in this Policy document, and to ensure that unacceptable use of Janet is dealt with promptly and effectively should it occur. The discharge of this responsibility includes informing all users of the Connected Organisation with access to Janet of their obligations in this respect (see Note 7).

20. Where necessary, service may be withdrawn from the Connected Organisation, in accordance with the Janet Terms. Where violation of these conditions is unlawful, or results in loss or damage to Janet resources or the resources of third parties accessible via Janet, the matter may be referred for legal action.

Explanatory notes

Note 1: The Acceptable Use Policy does not make any particular statement as to the acceptability of using Janet for activities resulting in commercial gain to the Connected Organisation, other than this is acceptable where lawful. However, it should be noted that there are legal constraints applying to a publicly funded Connected Organisation in such activities. Where the Connected Organisation is operating as an economic undertaking the issue of State Aid will need to be considered. There is also an issue of the status of both Janet and the User Organisation's network as private networks. Both are addressed in the Janet Network Connection Policy.

Note 2: It is preferable for misuse to be prevented by a combination of responsible attitudes to the use of Janet on the part of its users and appropriate disciplinary measures taken by their Connected Organisations.

Note 3: The list of unacceptable activities in this section is not exhaustive. The purpose is to bring as clearly as possible to the reader's attention those activities most commonly associated with the abuse and potentially unlawful use of a network.

Note 4: It may be permissible for such material to be received, created or transmitted where this is for properly supervised and lawful purposes. This may include, for example, approved teaching or research, or the reception or transmission of such material by authorised personnel in the course of an investigation into a suspected or alleged abuse of the institution's facilities. The discretion to approve such use, and the responsibility for any such approval, rests with the Connected Organisation. Universities UK has provided guidance on handling sensitive research materials.

Note 5: Implicit authorisation may only be presumed where a host and port have been advertised as providing a service (for example by a DNS MX record) and will be considered to have been withdrawn if a complaint from the provider of the service or resource is received either by the Connected Organisation or by Jisc. For all other services and ports, access will be presumed to be unauthorised unless explicit authority can be demonstrated.

Note 6: Where a Connected Organisation wishes to commission or itself perform a test for vulnerabilities in its IT systems (for example, via "penetration testing") this, as an action authorised by the Connected Organisation, will not be a breach of clause 15. However, the User Organisation should inform Jisc CSIRT, in advance of the test, of the source, nature and timing of the test. This is to avoid wasting the time and resources of Jisc CSIRT in investigating the perceived attack on the Connected Organisation, or automatically blocking it. Jisc CSIRT should be contacted via the details at https://www.jisc.ac.uk/csirt.

Note 7: In order to discharge this responsibility, it is recommended that each Connected Organisation establishes its own statement of acceptable use within the context of the services provided to its users. This should be cast in a form that is compatible with the provisions of this Acceptable Use Policy. Such a statement may refer to, or include material from this document. If material is included, this must be done in such a way as to ensure that there is no misrepresentation of the intent of the Janet Acceptable Use Policy.

[1] GEN-DOC-009 will be superseded in 2022 by the Master Services Agreement for Janet Connection Services

fircroftcollege