Acceptable Use Policy

Approving committee:	Information Governance Committee
Minute reference:	IGC/05/20/07
Document owner:	Information Technology - IT Security
Key Contact(s):	Jonathan Monk; Mike Roberts
Date of Equality Impact Assessment:	31/01/2020
Equality Impact Assessment Outcome:	No impact
Latest review date:	28/06/2024
Next review date:	27/06/2025

Acceptable Use Policy

Approving committee: Information Governance Committee
Minute reference: IGC/05/20/07
Document owner: Digital Services - Information Security
Key Contact(s): Jonathan Monk; Janine Terry
Date of Equality Impact Assessment: 31/01/2020
Equality Impact Assessment Outcome: No impact
Latest review date: 28/06/2024
Next review date: 27/06/2025

Table of Contents

1. Version Control

Version	Revision Details	Author	Date
1.0	First Signed Off Version	Chris Manley	10.06.20
1.1	Minor revision, correction of typos	Mary Dziorny	08/04/2021
1.2	Updated to reflect latest Digital Services structure and revise links to other policies	Kate Stewart	27/06/2024

2. Approval Details

Approving committee:	Information Governance Committee
Minute reference:	IGC/05/20/07
Document owner:	Chief Information Officer
Key Contact(s):	Chief Information Officer; Head of Digital Technologies
Date of Equality Impact Assessment:	30/01/2020
Equality Impact Assessment Outcome:	Agreed and granted acceptance 31/01/2020
Latest review date:	10.06.2020
Next review date:	10.06.2021

3. Introduction

The ICR is committed to protecting the confidentiality, availability and integrity of its information assets to safeguard its reputation and fulfils its legal, contractual and regulatory obligations.

The keywords below are used throughout this policy.

Key Word	Definition
Users	Any person(s) granted access to ICR data, networks, applications, equipment or premises including: staff, corporate staff, furloughed staff, honorary appointments, temporary workers, students, interns and volunteers.
Assets	ICR Information, Data, systems, networks, equipment and resources
Systems	ICR IT Applications, equipment and networks
Must / Shall	Mandatory
Must not/ Shall not	Prohibited
Should	Recommended, but implications are to be considered before execution
Should not	Not recommended, the implications are to be considered before execution
May	Optional

4. Purpose and Scope

This Policy defines the acceptable and unacceptable use of the ICR's information, resources and systems (hereafter referred to as Assets).

It is applicable to all individuals with access to ICR assets including staff, students, honorary appointments and temporary workers (hereafter referred to as Users).

It is applicable to all ICR sites including remote access working. Adherence to this Policy is mandatory to protect the ICR, its staff and its reputation from damage, either knowingly or unintentionally.

It is also applicable to entities that provide IT or technological infrastructure (i.e. hardware, software, services, research equipment) to ICR including any business units/functions within the ICR, including scientific departments and units.

It is the responsibility of all staff to familiarise themselves with this policy, and to conduct their activities accordingly. Failure to comply could result in disciplinary action including suspension, dismissal, and civil or criminal proceedings.

5. Background

The Acceptable Use of ICR Assets is a key factor in the maintenance of effective information security and the ICR sets clear principles by which users can conduct their activities.

Unacceptable use of ICR Assets exposes the ICR and its partners to risks including malware attacks; compromise of networks, systems and services; loss of intellectual property and sensitive information; and potential legal and regulatory breaches.

Whilst some activities can be restricted by technology, the ICR places its trust in the user to correctly use the resources that have been provided for them. This policy sets out the direction and principles that users must adhere to when using ICR Assets.

6. Policy

6.1. Universal Use

Where ICR users are allowed access to systems, they are expected to use it appropriately and in such a manner that does not interfere with the efficient running of the ICR.

Below are the principles by which the ICR expects its users to abide by.

6.1.1. Users **may** be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., system administrators **may** have a need to disable network access if a PC is disrupting services, or security **may** undertake vulnerability testing).

6.1.2. Whilst connected to the ICR's network, users are subject to **all ICR policies** that are in effect, regardless of their own physical location.

6.2. Prohibited Activities

6.2.1. Users **must not** engage in any activity that is **illegal** under UK or international law (as applicable) including, but not limited to: sexual harassment, fraud or hostile workplace laws.

6.2.2. Users **must not** use ICR systems to promote any activity that is likely to violate the relevant anti-discrimination law and/or ICR policy or incitement to hatred including, but not limited to discrimination: on the grounds of race, ethnicity, gender, sexual orientation, disability and religious beliefs.

6.2.3. Users **must not** view, send or forward any content that is: defamatory, discriminatory, obscene or otherwise inappropriate, or contains offensive material. This includes, but is not limited to: pornographic websites, videos or images; websites, images or other material related to extremist social; political or religious causes (or fall under the ICR's PREVENT duty); movements or ideologies. Contravening this will be treated as misconduct under the appropriate HR and disciplinary procedures.

6.2.4. Users **must not** use ICR systems to create, send or view any content or activity that may harm or be detrimental to the reputation of the ICR or bring it, its staff, students or partners into disrepute. This includes, but is not limited to: photographs, text (electronic or printed), audio and video files.

6.2.5. Users **must not** send or forward unsolicited content, including the sending of junk mail, chain letters and pyramid schemes, or other advertising material to individuals or internet groups including (but not limited to): Social media platforms, internet forums and bulletin boards; who did not specifically request such material (email spam) or making fraudulent offers of products, items, or services originating from any ICR account.

6.2.6. Users **must not** look at, change or use another person's data, systems, or equipment for which they do not have the owner's explicit permission, even in jest.

6.2.7. Users **must not** reveal any account passwords to others or allow use of your account by others. This includes colleagues, family and other household members.

6.2.8. Users **must not** provide information about, or lists of, ICR users to parties outside the ICR, without the required permissions or authorisation.

6.2.9. Users **must not** attach any non-approved equipment to ICR equipment or systems. Any requests for such actions **shall** be subject to risk assessment by Information Security.

6.2.10. Equipment or software **must not** be taken off-site by users without prior authorisation and (where appropriate) the completion of the Removal of ICR Owned Equipment Form. (Permission and provision of remote working is considered as authorisation for such devices).

6.3. Mandatory Activities

6.3.1. Users **must** check that the recipients of emails are correct when creating, replying to or forwarding any emails. (E.g. there **may** be cases where "reply all" is not appropriate). Extra care **must** be exercised when sharing RESTRICTED information via email, as doing so **may** result in disclosure of confidential information to the wrong person.

6.3.2. Users **must** exercise extreme care when receiving emails with attachments from third parties, particularly unidentified third parties, as these **may** contain viruses. If in doubt of the legitimacy of any email, you **must** contact the IT Service Desk.

6.3.3. ICR information stored on electronic and computing devices whether owned or leased by ICR or provided by an ICR client or a third party, remains the property of ICR. All users **must** ensure that ICR information is protected and managed throughout its life in accordance with all ICR policies, any applicable client or partner Non-Disclosure Agreements (NDAs) and contracts, and any applicable legislation.

6.3.4. Users are responsible for any ICR asset in their possession and should take reasonable care to minimise the risk of loss, theft or damage to ICR equipment in their possession. This includes the physical security of the hardware and the information it holds, at all times, both on or off ICR premises.

6.3.5. All devices on loan **must** be returned when users leave the employ of ICR.

6.3.6. ICR users **must** adhere to the ICR'S Information Classification Policy (See Appendix 2 – Classification System) when handling, transmitting and sharing any ICR data and information, through ICR systems.

6.3.7. ICR Information **must** be acquired, handled, processed, stored, maintained, transmitted, transferred and destroyed in accordance with the latest versions of ICR Policies and Procedures, unless superseded by legislative or regulatory requirements.

6.3.8. Users should be aware of their surroundings when conducting ICR business and be careful not to reveal sensitive or proprietary ICR information in an environment where it could potentially be overheard or seen.

6.3.9. Users **must** report the theft, loss or unauthorised disclosure of ICR assets immediately in accordance with ICR Information Security Incident Policy procedures.

6.3.10. Line managers, primary supervisors or system owners **must** inform system administrators when access rights are no longer required or justified on business grounds, so that access can be revoked.

7. Technical Policy

7.1. Technical Compliance

7.1.1. Compliance with the technical security requirements for systems are **mandatory** and users **must not** attempt to circumvent any measures, for any systems and networks in place.

7.2. Disruptions to Services

7.2.1. Users **must not** knowingly cause a security breach or disruption to ICR Systems.

7.2.2. Security breaches include, but are not limited to: accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorised to access, unless these duties are within the scope of regular duties.

7.2.3. "Disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes. The only exemption to this is when the user is on official ICR business conducting IT Health Check duties, penetration testing or training on a test network.

7.2.4. Users **must not** use or deploy any hacking, testing tools (hardware and software), or introduce malicious programs into the network (e.g. malware, key loggers etc.) intending to disrupt, circumvent or disable security measures or access unauthorised data on and / or from ICR systems.

7.2.5. No user is permitted to carry out any form of network monitoring which will intercept data not intended for the user's system, unless this activity is a part of the user's normal job/duty.

7.2.6. Circumventing user authentication of any host, network or account is **prohibited**. This includes, but is not limited to: reconfiguration of security features (e.g. collection or amendment of audit logs) and changing of passwords or permissions, unless it is part of professional duties.

7.2.7. No user **shall** introduce honeypots, or similar technology on the ICR networks unless prior notification has been given by the CIO (or an appointed delegate) and written authorisation has been obtained in advance.

7.3. Messages

7.3.1. Unauthorised use, or forging, of email header information or email addresses is **strictly prohibited.**

7.3.2. User **must not** deploy or use any program, script or command, or send messages of any kind, with the intent to interfere with, or disable, a user's session or access, via any means, locally or via the Internet/Intranet.

7.3.3. Users **must** report any malfunctions, irregular behaviour or suspected malware infection of any systems to the IT Service Desk as soon as possible.

8. Physical Media

8.1. Handling

8.1.1. Users **must not** use any unauthorised storage devices (including but not limited to: USB flash drives, flash memory cards (e.g. SD, Compact Flash, Micro SD and XD), USB hard drives, to connect to any ICR devices or store ICR data.

8.1.2. Users **must not** remove any RESTRICTED information (including research data) from ICR premises without the correct authorisation, technical protection (e.g. encryption) on digital media and handling procedures in place. Any portable device or memory card that is used to store sensitive ICR data **must** have an ICR approved encryption solution in place.

9. Software

9.1. Sourcing

9.1.1. ICR users **must** only download files from legitimate sources, to computers running virus-checking software. If in doubt, consult your line manager or the IT HelpDesk.

9.2. Installation

9.2.1. Software **must not** be installed on ICR IT systems (including ICR issued laptops and desktop computers) without authorisation from a line manager or the Information Security Team. Such installations **must** be in accordance with the ICR's software licensing policy, unless the installation is part of the user's role.

9.2.2. All software that ICR users install on ICR systems (including apps) **must** meet the following requirements:

- Be obtained legally, from a trusted source;
- Are supported by the manufacturer and have security updates applied in a timely manner
- Does not contain any known security vulnerabilities.

9.3. Intellectual Property

9.3.1. Software installed **must not** violate the rights of any person or organisation(s) protected by copyright, trade secret, research agreement, patent or other intellectual property, or similar laws or regulations.

a. Unauthorised copying of copyrighted material including (but not limited to): digitisation and distribution of photographs from magazines, books or other copyrighted sources (including downloaded content) and copyrighted music is strictly prohibited.

9.3.2. The loading, distribution and use of unlicensed software, including "pirated" software that is subject to copyright is **strictly prohibited**. Licensed software **must** be used in accordance with any End User Licence Agreement (EULA) and Service Level Agreement (SLA).

b. Open Source software **may** only be installed and used in accordance with any applicable Open Source licence, including any obligations contained therein.

9.3.3. If users are unsure of the above requirements, they must consult the Information Security Team for guidance.

10. Remote Working

10.1. General

10.1.1. Work **must** only be undertaken remotely using ICR equipment, or authorised remote access methods, unless otherwise authorised.

10.1.2. During transport, ICR assets **must** be: kept out of sight, kept secure at all times, and not left unattended at any time during the journey including being left in vehicles.

10.1.3. Users **should** take reasonable steps to secure all ICR assets in their home.

10.1.4. Users **should** take all reasonable steps to minimise the visibility of the screen and information on it when working off-site.

10.1.5. Users **must** use approved remote access methods to access ICR services. (See Nexus for details).

10.1.6. Critical data **must** be backed up to ICR storage at the earliest opportunity. RESTRICTED data including, but not limited to: commercially sensitive and special category personal data **should not** be stored solely on a machine's local drive, unless no connection is available when it is created.

11. Wi-Fi

11.1. Internal

11.1.1. Users **must** only use the ICR provided wireless networks when using ICR assets when on ICR premises.

11.2. External

11.2.1. Only where such services are unavailable **may** alternative wireless networking arrangements be allowed, subject to the following requirements being met:

a. The hosting and identity of the wireless access point is known to the user (e.g. home Wi-Fi or tethered to a phone) and **should** not be a communal or public access point.
b. Technical security requirements set out by the ICR must be used.

11.2.2. No unauthorised wireless access points of any kind or networking facilities connected to ICR systems or any ICR networks **shall** be permitted.

12. Third Party Use of Devices

12.1. General

12.1.1. Any personal or third party device required to store ICR data **must** have pre-approval from Information Security.

12.1.2. Any user wishing to access ICR information or systems (e.g. utilise web mail or receive email on a phone) **must** use the approved ICR technical controls and adhere to the technical requirements set out by Information Security.

12.2. Removal of Data

12.2.1. The ICR reserves the right to request that a user remove any and all ICR data from any personal device that **may** store it (e.g. where a user can access emails on their personal phone, they must remove all emails and settings when requested to do so).

12.2.2. Where a user cannot or refuses to remove ICR data from a personal device, using the approved ICR technical controls, where possible, the ICR **shall** action remote removal of the information.

13. Personal Use

The ICR allows a degree of personal use of its systems, which includes: browsing the internet; accessing personal email accounts; accessing personal cloud storage and social networking sites (e.g. social media platforms and forums).
When engaging in personal use of ICR systems, users **must** adhere to the following principles in addition to those above:

13.1. General

13.1.1. There are no time limitations on non-work use. Users are trusted **not to abuse** the latitude given to them, but if this trust is abused ICR reserves the right to alter the policy in this respect. **Personal**

usage is a privilege and not a right. In the event of any uncertainty, users must consult their line manager or supervisor.

13.1.2. ICR users **must not** use their work email address to register for non-work related activities. This includes, but is not limited to: online shopping accounts, online marketplaces, social media platforms, internet forums.

13.1.3. Users **shall** only use work issued email addresses to register for work related accounts and activities. They **must not** register or authenticate with personal email addresses.

13.1.4. Accessing ICR data for any purpose other than conducting ICR business, even if authorised access has been provided, is prohibited.

13.1.5. Users **should not** download any attachments from personal accounts on to ICR systems or equipment, unless authorised to do so; there is an overriding business need and other technical options have not been explored. Technical protection must not be circumvented in these cases.

13.1.6. Whenever users state an affiliation to the ICR and they are not officially authorised to communicate on behalf of the ICR, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the ICR" or similar.

13.2. Personal Cloud Services

13.2.1. Users **must not** transmit or store ICR Data on their personal cloud drive.

13.2.2. Users **must not** download information or data from their own personal cloud drive to ICR systems.

14. Social Media

14.1. Personal Social Media Use

14.1.1. Users **may** associate themselves with their employment at the ICR on social media networks and online platforms. However, they **must** be aware that they **must not** bring the ICR or its reputation into disrepute through any such association.

14.1.2. Users **must** take care not to attribute personal statements, opinions or beliefs to the ICR, unless officially representing the ICR.

15. Monitoring

15.1. General

As part of security best practices, the ICR carries out regular monitoring* of its Systems and Assets according to the following principles:

15.1.1. Users do not have any absolute right of privacy when using ICR systems.

15.1.2. For security and network maintenance purposes and as part of the ICR's PREVENT duties and obligations; authorised individuals within the ICR may monitor systems and network traffic at any time. Monitoring of a user's email and internet use shall be conducted in accordance with applicable laws and regulations.

15.1.3. Monitoring is in the ICR's legitimate and legal interests (e.g. PREVENT) and is to ensure that this policy is being complied with.

15.1.4. Monitoring for legitimate purposes may result in the capture of personal data including authentication credentials. The ICR are not liable for any personal damages or losses resulting from personal usage of their systems by users.

15.1.5. Any monitoring will normally be conducted by the ICR's Information Security team. The information obtained through such monitoring may be shared internally, including with members of the HR team, the user's line manager, and managers in the relevant business area and with IT users if access to the data is necessary for performance of their roles. However, information will only normally be shared in this way if the ICR has reasonable grounds to believe that there has been a breach of the rules set out within this policy.

15.1.6. The results of monitoring may form a part of the auditing, reporting and accounting requirements of the ICR and may be used in any investigation.

15.1.7. Information obtained through monitoring shall not be disclosed to third parties, unless the ICR is under a duty to report matters to a legal or regulatory authority or to a law enforcement agency.

15.1.8. ICR system logs are retained for a minimum of 90 days or in line with contractual, regulatory and legal requirements.

15.1.9. The ICR reserves the right to block any activities that are deemed unsuitable or that contravene this policy, are deemed to be in contravention of existing or future legislation (e.g. PREVENT), future ICR policies and / or which pose a direct technical threat to the ICR systems.

*Official investigations and associated activities, not limited to extraordinary monitoring, evidence gathering, interviews and potential restrictions in use of data and systems, are governed by the HR department and **shall** be actioned on a case by case basis. Regular monitoring activities **may** precipitate or feed into such activities

15.2. Re-possession of Equipment

15.2.1. The ICR has right to re-possess or take possession of any ICR equipment issued to any user at any time and for any reason. This may include (but is not limited to): suspected malware infection, hardware or software malfunctions, suspected misuse of assets and potential PREVENT requirements.

15.2.2. (Note: repossession of equipment is not an indicator of any wrongdoing or misuse; however, the ICR does not have to give an individual a reason for recovering a machine.)

15.2.3. The ICR reserves the right to inspect assets on a periodic basis to ensure compliance with the ICR policies and it's PREVENT duties and obligations.

15.3. Examination of Data and Equipment

15.3.1. The ICR **shall** conduct any level of examination on any ICR assets, as it deems necessary.

15.3.2. The ICR **shall** follow strict forensic handling procedures and processes in the examination of assets, where deemed necessary.

15.3.3. Record and documentation **shall** be retained around any action where assets are re-possessed and examined.

15.3.4. The ICR **shall not** pass on any data that is recovered or examined, as part of an investigation, to third parties unless it has a duty to report matters to a regulatory authority or law enforcement agency.

16. R.A.C.I Matrix

The roles listed below have the following interests in this policy/process:

Responsible	All users
Accountable	Executive Board
Consulted	HR, IT, Communications, Digital, Staff Side
Informed	All

17. Policy Compliance

17.1. General

17.1.1. Compliance with ICR policies and procedures is mandatory for all users of ICR systems.

17.1.2. Any breach of this policy **must** be reported to Information Security Team as soon as possible. This reduces wasted resources spent on investigations and helps develop better controls.

17.1.3. If a user suspects someone of intentionally misusing ICR systems, equipment or data, they **must** report this to their line manager and the Information Security Team. Any such reports will be treated in the strictest confidence and **shall not** be divulged unless there is a legal, regulatory or duty of care requirement identified

17.1.4. Compliance with this policy will be monitored on a regular, ongoing basis and any non-compliances will be investigated. Corrective action will be taken where deemed necessary by Senior Management and the relevant stakeholders, as part of a continuous service improvement programme.

17.1.5. Non-compliance with ICR policies and procedures could result in:

· Disciplinary action being taken against an individual in accordance with their contract of employment, the ICR Disciplinary Policy and Procedure, and the ICR Academic users - Dismissal, Discipline, Grievance Procedures and Related Matters, up to and including dismissal.
· The Student Disciplinary Process being carried out in the event the potential breach is committed by a student.
· Legal and criminal action against the individual.

17.2. Exceptions

It is recognised that some activities conducted by the divisions, directorate or individuals within the ICR require exceptions to this policy.

Where there is an explicit business need, there shall be a process and record of the justification, including approval authority. This may be in any written format, and a copy of the authorisation should be kept by the user.

The requirements should be reviewed regularly, no less than annually, and the users that are covered by the exception shall notify the relevant department, in writing, when the exception is no longer required.

For the basic process, please see Appendix 1 – Policy Exception Process.

18. Appendix 1 – Policy Exception Process

19. High Level Process

In the event that a user requires an exception for this policy, they must apply for a policy exception with the following process:

1. Upon identifying that there may be a requirement for a policy exception, the user should identify the following:
· A clear business case as to:
· Why they require the exception
· What the scope of the exception is (e.g. what material they will be viewing, and whether they think they need technical considerations)
· The policy and clause(s) that may be in violation.

2. Once the information on the exception has been prepared, the user should check whether an exception with the same details has previously been granted. This could be to a colleague, or previous user, or potentially to the user himself or herself.

3. If the exception has been granted, the user should check whether 1 year has elapsed since approval.

a. If it is under a year, then the exception is still valid and the user may continue to work (END PROCESS).

b. If the exception was granted over a year ago, proceed to Step 4.
c. If no exception has been granted, proceed to Step 4.
4. The user should consult their line manager and discuss the need for an exception to the policy.
5. Between them, they should try to agree and identify the breach of the policy and need for the exception.
a. If they cannot, they should seek advice from the department that owns the policy.
6. Once a valid exception has been identified, the user should fill out a policy exception form.
7. The form will be sent to the Deputy Director* of the department the user works for, for review.
a. If the Deputy Director signs the exception off, the form will be sent to the Chief Information Security Officer* (CISO) for review.
b. If the Deputy Director does not issue sign-off, the user should consult with their line manager

before resubmission.
c. If the CISO does not issue sign-off, the user should consult with their line manager before resubmission.

* If the signatory chooses to, they may also seek approval from other departments (e.g. Information Governance).

8. Once the CISO has granted approval, the user and Information Security shall maintain a record of the exception.

20. Appendix 2 – Classification System

ICR - Classification System Identifier		Definition
DEF-001 - Public Information		Public Information is intended for general external publication, such as information ICR must or wishes to publish on its website. There are two sub-categories of Public Information – Regulatory and Non-Regulatory.
	DEF-001A - Regulatory	Refers to information that ICR is required to publish under current legislation.
	DEF-001B - Non-Regulatory	Refers to information that ICR has prepared for publication and wants to publish.
DEF-002 - Internal Information		Internal Information includes internally generated information that is not intended for public consumption, and that does not contain any Restricted information.
DEF-003 - Restricted Information		Restricted Information is information that ICR intends to (and may be legally required to) keep confidential. There are two sub-categories of Restricted Information – regulatory and non-regulatory.
	DEF-003A - Regulatory	"Restricted Information – Regulatory" refers to information that ICR has a statutory or contractual duty to protect from third party access or publication.
	DEF-003B - Non-Regulatory	"Restricted Information – Non-Regulatory" refers to information that the ICR chooses to restrict access to for its own purposes.

For full details, please see Nexus for the full ICR Information Classification Policy.

Approved ICR policy