Diamond IT Acceptable Use Policy	
Version/Date:	Version 0.5 / 5 July 2021
	Version 0.4 / 14 June 2021 – further input from ERC
	Version 0.3 / 1 June 2021 -- submitted to ERC for comment
	Version 0.2a / 15 May 2021 – circulated to Information Technology Governance Committee
	Version 0.2 / 12 May 2021 – circulated to Information Governance Work Group
	Version 0.1 / 5 May 2021 – initial version
Reference/Status:	Version 0.5
Access:	'Public'
Author	P.W. Jeffreys

Diamond IT Acceptable Use Policy

The Diamond IT Acceptable Use Policy (IT AUP) is part of a suite of Information Technology and Information Governance policies listed in the Information Technology Information Governance Framework document. Its primary aim is to enable appropriate, effective and efficient use of systems, services and facilities at Diamond.

1. Policy Statement

Diamond Information and Communication Technology (ICT) systems, services and facilities are provided to enable individuals, as defined in section 2, to use facilities appropriately, effectively and efficiently. All normal use of these systems, within an individual's authority to act in pursuit of Diamond business, is allowed.

The purpose of this Policy is to identify proper usage and behaviour of individuals using Diamond ICT systems and services. It should be read in conjunction with the Information Technology Information Governance Corporate Statement.

The Policy sets common standards of ICT acceptable use. Where additional organisational or project standards of acceptable use are set, these must be consistent with the standards set by this Policy and documented separately. Sensitive or personal information must be appropriately protected in line with other relevant Diamond Policies.

All parties are expected to conduct themselves in line with Diamond's Values and Behaviours of Respect, Excellence, Collaboration, Integrity and Innovation.

The IT AUP replaces an 'IT Users Guide and Policy', dating from January 2010, available from the Intranet, and not designed for the broad range of different types of user defined in Section 2.

2. To whom does this Policy apply?

This document must be read and adhered to by those listed in the Information Technology Information Governance Framework, namely: all individuals working for Diamond or on our behalf in any capacity, including: Diamond Employees, joint appointees, seconded workers, collaborators, members of advisory groups/committees, members of review panels, students, volunteers, interns, agents, contractors (specifically including suppliers and casual and agency staff), external consultants, third-party representatives and facility users.

3. Who is responsible for this Policy?

Diamond's Directors have overall responsibility for this policy. The Directors have delegated day-to-day responsibility for its operation to the Head of Cyber Security and Information Governance.

4. Compliance with other policies, regulations and procedures

This policy should be read in conjunction with the Data Protection Policy, and any privacy notices that Diamond may communicate.

5. IT Acceptable Use Policy Principles

- Diamond's ICT services can be put at risk through improper or ill-informed use and result in consequences which may be damaging to individuals and their research, Diamond operations, the Diamond community and its reputation.
- The Policy aims to provide clear information concerning the use of Diamond information, information systems and software in all forms. It provides a framework to:
    - Enable individuals to use Diamond facilities securely and with confidence;
    - Help maintain the security, integrity and performance of Diamond systems and services;
    - Minimise both Diamond's and individual users' exposure to possible legal action arising from unauthorised use of the systems and services;
    - Minimise Diamond and individual users' exposure to unauthorised, excessive or inappropriate expense through business related activities;
    - Help ensure that Diamond can demonstrate effective and appropriate use of publicly funded resources; and,
    - Set a standard for acceptable use across all Diamond systems and services.
- It is Diamond's responsibility to ensure that individuals have access to this Policy. It is each individuals' responsibility to read, be fully familiar with, and abide by this Policy and also the Joint Information Systems Committee (JISC) Acceptable Use Policy[1].
- Sensitive or personal information must be protected appropriately in accordance with the Diamond Data Classification policy. Security classifications indicate the sensitivity of information (in terms of the likely impact resulting from compromise, loss or misuse).

6. Breach of this Policy

Examples of unacceptable activities are given below in this Section; this list is not exhaustive. Breaches of the Policy may:

- In the case of Diamond Employees, result in disciplinary action up to and including dismissal depending on the nature and severity of the breaches.
- In the case of individuals who are not Diamond employees, result in termination of any contract that they may have in place with Diamond and/or termination of their current and future access to Diamond.

[1] The Jisc AUP covers electronic communications network and associated electronic communications networking services and facilities that support the requirements of the UK education and research communities.

The following activities are unacceptable:

6.1. Transmitting, downloading or storing any material such that infringes the copyright of the owner.
6.2. Deliberately creating, storing or transmitting information which infringes the data protection registration of Diamond.
6.3. Purchasing goods or services or entering into any contract on behalf of Diamond without necessary authority.
6.4. Business advertising or trade sales.
6.5. Trading, i.e. sale of any goods purchased with the sole intention of making a profit.
6.6. Unauthorised redistribution of email.
6.7. Sending or forwarding chain emails.
6.8. Making your personal username and password (also known as a 'user account') available for other individuals to use on your behalf.
6.9. Allowing other individuals to use your device under your own user account without supervision.
6.10. Accessing information, systems or services without appropriate authorisation or using another's credentials (beamline workstations are excluded from this).
6.11. Knowingly allowing the use of Diamond system, services and resources by unauthorised third parties.
6.12. Disabling, altering bypassing or circumventing any measures put in place by Diamond to maintain the safe and secure operation of systems, services and information. This includes non-cooperation with investigations or audits.
6.13. Misrepresenting Diamond by unauthorised or inappropriate publishing. For example, blog posts, tweeting.
6.14. Failing to follow Diamond requirements on how to protect, store, transmit, share and access information both within and outside Diamond.
6.15. Inappropriate messaging to large groups of users. For example, sending non-work-related emails to all employees.
6.16. Using another person's log on details (username and password).
6.17. Using software that is not appropriately licenced.
6.18. Attempting to gain or facilitate unauthorised access to a computer system, service or information.
6.19. Attempting to or deliberately corrupting, destroying or denying access to another user's email, data files, information, system or service.
6.20. Deliberately accessing, viewing, receiving, downloading, sending or storing material that:

6.20.1. promotes or encourages discrimination, racism or intolerance;
6.20.2. is illegal in the UK;
6.20.3. is defamatory, threatening, harassing, offensive or abusive;
6.20.4. will, or is likely to, bring Diamond its employees or partners into disrepute;
6.20.5. is known to be infected with a virus, worm, Trojan or any form of malicious software or code;
6.20.6. infringes the privacy and data protection rights of individuals;
6.20.7. could endanger the health and safety or wellbeing of any other individual.

Individuals may be exposed to unsolicited receipt of content, or accidentally view illegal material:

- Unsolicited receipt of discriminatory, abusive, pornographic, obscene, illegal, offensive or defamatory messages (e.g. email SPAM / text messages) must be reported to the Diamond Information Security Team[2].
- Anyone accidentally viewing what they believe is illegal material (e.g. indecent images of children) must immediately stop what they are doing, take a note of where they found the illegal material and close the software application displaying the material; this includes email. The individual must not view

[2] This links to the IGC email account, 'Information Governance Centre'

the illegal material again and must take appropriate measures to ensure that others cannot view the material. They must immediately inform their line manager, or Diamond host, and send an email to the Diamond Information Security Team, who will advise how to proceed. It may be a criminal offence to continue to view, allow others to view, or not to report illegal material and as such Diamond may be required to report the matter to the police or appropriate authorities.

7. Monitoring ICT Services by Diamond

- Diamond/STFC employs monitoring techniques on ICT systems and services, including email and Internet access, to enable the continuous improvement of services, detection of illegal activity, and to ensure that these facilities are not being misused.
- Monitoring is limited to the minimum data to fulfil the purpose of the monitoring activity (e.g. security, performance tuning) and will never include gathering of personal information unless specifically instructed to do so by the Executive. Processing is most often through the use of automated tools and access to the logs is restricted to authorised personnel: the Information Security Team or system administrators given this responsibility by the Executive. Investigations of suspected abuse would only be conducted when authorised by the Senior Information Risk Owner[3] (or a person with delegated security responsibility), and carried out by appropriately trained employees.
- Diamond subscribes or uses services provided by third parties (e.g. Microsoft, STFC). These parties may also monitor the access and use of those services to protect them from unauthorised access, improve their service offerings or to determine payment charges.
- Since Diamond is liable for data on its systems and services, it reserves the right, as part of any investigation, to inspect the contents of any emails (to diamond.ac.uk) accounts, or any other form of communications that are sent or received, and of Internet sites accessed, to check for compliance with this Policy.

8. Personal files, documents and emails

- Whilst Diamond takes steps to ensure the security of all information held on its services, it is not liable for such information stored on its systems should it be lost, destroyed or accessed inappropriately.
- Wherever possible, employees responsible for monitoring or inspecting the systems and services will respect emails and folders which are marked ‘Personal’ or ‘Private’; the only exceptions will be when directed by the Executive.
- At management discretion, Diamond employees are allowed limited and reasonable personal use of Diamond systems and services provided that such use does not:
    - interfere with normal work or the work of others;
    - involve more than minimal amounts of working time;
    - incur any unauthorised expense for Diamond and/or tie up a significant amount of resource;
    - involve access to offensive or illegal material, such as material containing racist terminology or which is sexually explicit;
    - result in illegal activity, expose Diamond to civil legal action, or risk bringing Diamond into disrepute;
    - include intentional use of software or techniques meant to disguise or circumvent detection of computing activities;
    - expose Diamond to additional risk or compromise Diamond’s technical integrity.
- Responsibility for ensuring that any personal use is acceptable rests with the individual.

[3] Diamond’s SIRO is the Director of Financial and Corporate Services

9. Use of Social Media

Diamond encourages the use of Social Media to enhance communication, collaboration, innovation and to engage with third parties in support of Diamond's objectives. A Social Media policy encourages good practice, clarifies where and how existing policies and guidelines apply to Social Media, promotes effective and innovative Personal Use of Social Media and Business Use of Social Media, whilst at the same time minimising any potential risk of damage, whether reputational or otherwise, to Diamond.

10. Exceptions

The nature of some forms of work might seem to contravene what would normally be considered appropriate use, for example the study of some medical research. Where this is necessary, it must be restricted to specific approved work identified as necessary for completion of that activity and security professionals consulted who will provide guidance appropriate to the activity and record the exception. Exceptions must be approved by the Information Technology Governance Committee.

11. Amendments to this Policy

This Policy will be reviewed every 2 years by the Information Governance Work Group to incorporate legislation or regulatory changes.

The current version of the Policy is dated 5 July 2021; version 0.5.