Information Security Policy

1. Policy Statement

The purpose of the Diamond Information Security Policy (the 'ISPolicy') is to set out Diamond's aims and objectives for the management of information security throughout the company. Information Security is defined as the preservation of confidentiality, integrity and availability of information.

The ISPolicy forms an integral part of an overall Information Security Framework (the 'Framework') as set out in section 5, which is designed to:

- Protect Diamond's information assets and technology against compromise of confidentiality, integrity and availability
- Support Diamond's Goals through a proportionate approach which balances usability and security.
- Facilitate a 'security aware' culture across Diamond and promote Information Security as everyone's responsibility.

2. Who does this policy apply to?

This document must be read and adhered to by those listed in the Information Technology Information Governance Framework document, 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 Cyber Security Lead.

4. Compliance with other policies, regulations and procedures?

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

5. Information Security Framework

Diamond's information security is managed through a Framework which comprises:

i. This and other policies that relate to information security;
ii. Compliance with information security standards, or parts of standards relevant to Diamond, including: Cyber Essentials, ISO/IEC 27001, CIS Critical Security Controls;
iii. Alignment of security operations with the NIST Cybersecurity Framework core functions of Govern, Identify, Protect, Detect, Respond, Recover;
iv. Information security governance – delivered through the Information Technology Governance Committee (ITGC), the Diamond Information Security Team, and associated Work Groups;
v. Management of security-related risk through Information Technology and Information Governance risk registers;
vi. Maintenance of a record of Cyber Security Alerts (the alerts record is accessible to users with diamond.ac.uk accounts);

vii. Fostering a culture of information security awareness, including training and best practice sharing across the organisation;
viii. Management and protection of personal data;
ix. Continuous improvement considering security trends and threat landscape, based on threat intelligence from authorities including the National Cyber Security Centre (NCSC).

The Framework provides a flexible and effective platform upon which the Diamond's information security objectives are met. Adherence to this Policy can be met by adopting and complying with the associated Standards.

6. Information Security Policy Principles

Diamond's Information Security Policy principles, embraced within the Information Security Framework, are:

- Diamond will protect the security of its information assets, in order to:
  - maintain the integrity and quality of information, so that it is accurate, up to date and fit for purpose;
  - make information available to those who need it and ensure there is no disruption to the business of Diamond;
  - ensure that confidentiality is not breached, so that information is accessed only by those authorised to do so; thereby ensuring that the Diamond meets its legal and regulatory obligations with respect to information handling, that business is conducted efficiently, that intellectual property is protected and that the reputation of Diamond is safeguarded.
- Diamond will manage the risks it faces in relation to information security, keeping its risk exposure to acceptable and proportionate levels. ITGC will include allocation of ownership of information security risks and information assets to provide accountability.
- Information security incident recording, reporting and management system will be implemented and monitored, with outcomes informing future risk assessments.
- Diamond will ensure that its information security framework is fit for purpose by utilising the NIST Cybersecurity Framework, and by benchmarking itself with respect to information security against comparator institutions, where possible.

Diamond users are required to:

- Read and engage with the ISPolicy.
- Complete Information Security Awareness Training as requested.
- Ensure that reasonable effort is made to protect Diamond's information and technology from accidental or unauthorised disclosure, modification or destruction.

7. Monitoring

Awareness of this policy forms part of Diamond's induction and training process.

8. Breach of the ISPolicy

Depending on the nature and severity, breaches of the Policy may:

- In the case of Diamond Employees, result in disciplinary action up to and including dismissal.
- 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.

8. Amendments to the ISPolicy

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 11 August 2025; version 1.1.

9. Definitions

For the purposes of this policy, the following definitions shall apply:

Availability: Having appropriate access to Information Assets as and when required in the course of Diamond's business

Confidentiality: The restriction of information to those persons who are authorised to receive or access it

Information*:* Data that has a meaning or can be interpreted. It can be held as an electronic record or in a non-electronic format such as paper, microfiche, photograph

Information Asset: Information that has value to Diamond. Key Information Assets are the most important types of information required for achievement of Diamond's strategic aims

Information Security: A systematic approach to managing information within a predefined acceptable range so that it remains secure. It includes people, processes and technology by applying a risk management process.

Integrity: The completeness and preservation of information in its original and intended form unless amended or deleted by authorised people or processes

Quality: The state of completeness, validity, consistency, timeliness and accuracy that makes data appropriate for both operational and strategic use.

Risk: The chance or possibility of uncertainty on objectives, expressed as a combination the probability of an event occurring and the impact such an event would have on the achievement of one or more objectives.

Document Control Table	
Policy Title:	Information Security Policy
Policy Owner:	Cyber Security Lead
Current Version and Version number:	1.1
Approved By:	Information Governance Working Group
Approved Date:	11.08.2025
Next Review Date:	11.08.2027