# Information Governance Framework

| | |
|---|---|
| **Approving committee:** | Information Governance Committee |
| **Minute reference:** | IGC/05/22/03 |
| **Document owner:** | Academic Services - Information Governance |
| **Key Contact(s):** | ; |
| **Date of Equality Impact Assessment:** | 19/07/2017 |
| **Equality Impact Assessment Outcome:** | No impact |
| **Latest review date:** | 04/05/2022 |
| **Next review date:** | 04/05/2025 |

**This document sets out ICR staff roles and legal obligations, and must be read and adhered to by all ICR staff and students, including those on Honorary Appointments and other temporary workers, students and third parties who process ICR information.**

**The ICR has a suite of information governance and information technology policies, procedures and guidance which all ICR staff must familiarise themselves with and must be followed to ensure that ICR information is managed effectively throughout its whole lifecycle.**

## 1. Introduction

This framework outlines the core principles which apply to the management of all ICR information. This includes creating, maintaining, storing, using, sharing, protecting, retaining, archiving and destruction of both hardcopy and electronic information. For clarity, the term *information* is used to describe any data and knowledge that is generated from that data and recorded in the course of ICR business; this includes personal data, images, voice and video recordings, general administrative documents, emails etc.

Information Governance (IG) covers the following key areas:

- Data Protection
- Records Management
- Information Security
- Freedom of Information

It is essential that all employees (including visiting workers and contractors) and research degree students of ICR:

- Manage ICR information in line with its classification
- Comply with ICR policies, procedures and guidance
- Complete the online mandatory training modules (outlined within the Information Governance Training Needs Analysis) and abide by these principles
- Give full and urgent cooperation when required to compile a response to an incident, subject access request or freedom of information request.

The purpose of this document is to set out the policies and principles by which The Institute of Cancer Research ensures information is:

- Held securely and in accordance with information classification
- Obtained and processed fairly and lawfully
- Recorded accurately and reliably
- Used effectively and ethically
- Shared and disclosed appropriately and lawfully
- Stored and backed up robustly in line with ICR policies
- Made available and its integrity is assured.

The key disciplines of Information Governance which influence and protect ICR information are introduced below.

### 1.1 Data Protection

The Data Protection Policy outlines our obligations as an organisation to respect an individual's confidentiality, and to ensure the safe use of personal data. While it is also important to protect ICR's interests the aim of data protection is to safeguard the individual (data subject) from harm and only use their personal data lawfully. The Data Protection policy outlines the key principles of data protection legislation which the ICR and our staff must comply:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

### 1.2 Records Management

Records management is defined as a field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including process for capturing and maintaining evidence of and information about business activities and transactions in the form of records.

The Records Management policy applies to all records created, received or maintained by ICR staff (including visiting workers) and students in the course of carrying out their functions on behalf of ICR. Records and documentation created in the course of ICR research, whether internally or externally-funded, are also subject to contractual record-keeping requirements.

Records are defined as all those documents which facilitate the business carried out by The Institute and which are thereafter retained to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy, physical form or electronically.

A small percentage of The Institute's records will be selected for permanent preservation as part of the organisation's archives, for historical research and as an enduring record of the conduct of business.

### 1.3 Information Security

Information security ensures the protection of information as well as identifying and acting on threats to its security. It assures business continuity, minimises the impact of security related incidents, and ensures the integrity of the information held by ICR. It enables information to be processed and shared with appropriate safeguards in place.

The ICR uses an information classification scheme (ICR Information Classification) which provides categories which help ICR staff determine how to manage information. The categories are Public, Internal and Restricted.

To protect information from all threats, whether internal or external, deliberate or accidental, ICR will ensure:

- Information is protected against unauthorised access
- Integrity of information is maintained
- Regulatory and legislative requirements are met
- Business continuity plans are produced, maintained and tested
- Information security training is mandatory for all staff
- All breaches of information security, actual or suspected, are reported in line with the Information Security Incident Policy.

### 1.4 Freedom of Information

The Freedom of Information (FOI) Act gives anybody the right to seek access to information held by a public authority. As such the ICR has a statutory responsibility to make certain information routinely available.

## 2. Information Sharing

Information sharing is a core part of the collaborative nature of research. It is important that information is shared only with the correct safeguards in place, where there is a lawful basis to do so and with the correct permissions from colleagues within ICR. The ICR Information Classification Guidance must be followed and, if personal data will be shared, the Sharing Personal Data under Data Protection Act Policy.

Some staff and students will carry out work and process information under the control of other organisations. Where this is necessary staff and students may be required to comply with relevant policies, procedures and training requirements of other organisations or standards may be set by a data sharing agreement. In these scenarios staff and students must ensure that they and the ICR can comply with any additional responsibilities placed upon them.

Under no circumstances must ICR staff or students agree to terms of processing that are below the standards set by ICR policies.

## 3. Relevant Legislation

ICR policies and procedures are drafted to reflect relevant legislation and are outlined below.

| | |
|---|---|
| Data Protection Act 2018 (UK GDPR) | The Data Protection Act 2018 controls how your personal information is used by organisations, businesses or the government. The Act seeks to empower individuals to take control of their personal data and to support organisations with their lawful processing of personal data.<br><br>The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR). |
| Freedom of Information Act 2000 | This Act provides public access to information held by public authorities. As a higher education |

| | |
|---|---|
| | institution, the ICR is a public authority under the Act. |
| Human Rights Act 1998 | This act sets out the fundamental rights and freedoms that everyone in the UK is entitled to. One of the rights is the right to respect for private and family life which must be adhered to when processing information that identifies individuals. |
| Computer Misuse Act 1990 | Makes provisions for securing computer material against unauthorised access or modification; and for connected purposes. |
| Health Service (Control of Patient Information) Regulations 2002 | These Regulations, made under the NHS Act 2006, enable the common law duty of confidentiality to be temporarily lifted so that confidential patient information can be transferred to an applicant without the discloser being in breach of the common law duty of confidentiality**.** |
| Privacy and Electronic Communication Regulations (PECR) | Give people specific privacy rights in relation to electronic communications. |

# 4. Governance, Roles and Responsibilities

All ICR staff and students are responsible for information they create, maintain and/or handle (including disposal) in line with ICR policy. Specific roles are outlined within the information governance roles and responsibilities on Nexus and all ICR staff and students must familiarise themselves with their own responsibilities.

### 4.1 Information Governance Committee (IGC)

The remit of the Information Governance Committee is to ensure that ICR information is managed legally, securely, efficiently and effectively in compliance with relevant regulations and ICR policy. The IGC terms of reference are available on Nexus.

### 4.2 Senior Information Risk Owner (SIRO)

The SIRO is an executive or senior manager who attends the Board of Trustees and is responsible for information risks and the organisation's response to risk, currently the Chief Research and Academic Officer (CRAO). The SIRO ensures that all risks receive the appropriate response and are dealt with promptly and efficiently.

### 4.3 Caldicott Guardian

The Caldicott Guardian is a senior person within the organisation who ensures that patient information is used legally, ethically and appropriately, and that confidentiality is maintained. The Caldicott Guardian is a member of the Information Governance Committee and provides expert knowledge to ensure the committee's decisions properly reflect the rights of the patients. The ICR's Caldicott Guardian is Professor Ros Eeles.

### 4.4 Data Protection Officer

The primary role of the Data Protection Officer (DPO) is to ensure that the organisation processes personal data in line with the applicable data protection legislation. It is a statutory requirement of GDPR for an organisation such as the ICR to have a DPO who is responsible for overseeing GDPR compliance. The DPO is responsible for escalating data protection concerns and risks to senior management and the SIRO. The DPO is the Head of Information Governace.

# 5. Training

All new starters (temporary contract or permanent) must pass the mandatory IG and IT Security training courses. Training needs are assessed annually and outlined within the ICR Information Governance Training Needs Analysis document. This is available on Nexus.

# 6. Audit and monitoring

### 6.1 Annual Information Asset Audit

The information asset audit is completed every year and coordinated by Divisional Information Asset Administrators. The audit is used to record where personal information is processed within ICR and is a statutory requirement. The audit results are used to create records of processing and identify any high risk areas.

### 6.2 Information Governance and Information Security Audits

High risk areas identified within the information asset audit will be prioritised for information governance and information security audits. These areas are audited annually.

Audit criteria are mapped against key information governance and information security policy statements: the purpose being to discover whether relevant policies have been followed and whether personal data has been put at risk. The audits comprise of spot checks, observations and access checks.

### 6.3 Monitoring

The IGC receive reports about any areas of non-compliance with policy identified by audits and suggested mitigations. Where necessary the IGC can record areas of non-compliance on the ICR Information Risk Register. High scoring risks are then escalated as per the ICR's risk management process.

# 7. Implementation and dissemination of document

This Framework is shared with all ICR staff and students on appointment, is referenced within mandatory training and is available via Nexus.

### 7.1 Enforcement measures

Failure to comply with the standards and appropriate governance and security of information as detailed in this framework, policies, procedures and guidance can result in disciplinary action. All ICR staff and students are reminded that this framework covers aspects of legal compliance that as individuals they are responsible for. Failure to maintain these standards could result in criminal proceedings against the individual.