Information Governance Framework and Policy

# Document Control:

| **Document Control Information** | **Details** |
| --- | --- |
| Policy Name | Information Governance Framework and Policy |
| Policy Number | MSEICB 010 |
| Version | 1.1 |
| Status | Approved Final Version |
| Author / Lead | Information Governance Lead |
| Responsible Executive Director | Director of Resources and Senior Information Risk Owner |
| Responsible Committee | Audit Committee |
| Date Ratified by Responsible Committee | 20 June 2022 |
| Date Approved by Board/Effective Date | 1 July 2022 |
| Next Review Date | 1 July 2024 |
| Target Audience | All ICB Board members and staff (including temporary/bank/agency/work experience staff, students and volunteers), contractors engaged by the ICS Body, Staff from other MSE ICS Partnership organisations (including those working within ICS Body facilities), Patients and members of the public (visitors, individuals on work experience). |
| Stakeholders engaged in development of Policy (internal and external)  | * Information Governance Team.
* Information Governance Steering Group.
* Audit Committee.
 |
| Impact Assessments Undertaken | * Equality and Health Inequalities Impact Assessment – completed.
 |

# Version History

| Version | Date | Author (Name and Title) | Summary of amendments made |
| --- | --- | --- | --- |
| 1 | 01.07.22 | Iain Gear, Information Governance Lead | First version of the policy |
| 1.0 | 06.07.22 | David Triggs, Governance Lead | Final checks |
| 1.1 | June 2023 | Iain Gear, Information Governance Lead | Review date amended to 2 years |

# Contents

[1. Introduction 5](#_Toc108013868)

[2. Purpose / Policy Statement 6](#_Toc108013869)

[3. Definitions 7](#_Toc108013870)

[4. Roles and Responsibilities 8](#_Toc108013871)

[4.1. All ICB Employees and Board members 8](#_Toc108013872)

[4.2. Integrated Care Board 8](#_Toc108013873)

[4.3. Chief Executive 9](#_Toc108013874)

[4.4. Senior Information Risk Owner (SIRO) 9](#_Toc108013875)

[4.5. Caldicott Guardian 9](#_Toc108013876)

[4.6. Head of Information Governance / Data Protection Officer (DPO) 9](#_Toc108013877)

[4.7. Information Governance Team 10](#_Toc108013878)

[4.8. Associate Director of IT 10](#_Toc108013879)

[4.9. Information Security Officer 10](#_Toc108013880)

[4.10. Information Asset Owners (IAOs) 10](#_Toc108013881)

[4.11. Information Asset Administrators (IAAs) 11](#_Toc108013882)

[4.12. Information Governance Steering Group (IGSG) 11](#_Toc108013883)

[5. Policy Detail 11](#_Toc108013884)

[5.1. Overarching Legislation and Principles 11](#_Toc108013885)

[5.2. Annual Information Governance Audit 13](#_Toc108013886)

[5.3. Mandatory Training and Awareness 13](#_Toc108013887)

[5.4. Confidentiality Code of Conduct 13](#_Toc108013888)

[5.5. Information Asset Management and Business Continuity 13](#_Toc108013889)

[5.6. Information Risk Management 15](#_Toc108013890)

[5.7. Records of Processing Activities 16](#_Toc108013891)

[5.8. Data Protection Impact Assessments (DPIA) 17](#_Toc108013892)

[5.9. InfoSec, Cyber Security and User Access Controls 17](#_Toc108013893)

[5.10. Safe Haven 18](#_Toc108013894)

[5.11. Records Management 18](#_Toc108013895)

[5.12. Contracts 18](#_Toc108013896)

[5.13. Processing Data, the Use of Consent, and Information Sharing 19](#_Toc108013897)

[5.14. Data Quality Assurance 20](#_Toc108013898)

[5.15. Subject Access Requests 20](#_Toc108013899)

[5.16. Disclosure of Information to the Police 21](#_Toc108013900)

[5.17. Information Governance, Infosec and Cyber Security Incidents 21](#_Toc108013901)

[6. Monitoring Compliance 22](#_Toc108013902)

[7. Staff Training 23](#_Toc108013903)

[8. Arrangements for Review 23](#_Toc108013904)

[9. Associated Policies, Guidance and Documents 23](#_Toc108013905)

[10. Equality Impact Assessment 23](#_Toc108013906)

[Appendix A - Equality Impact Assessment 24](#_Toc108013907)

[Appendix B – Senior Information Risk Owner Role 27](#_Toc108013908)

[Appendix C – Caldicott Guardian Role 28](#_Toc108013909)

[Appendix D – Data Protection Officer Role 29](#_Toc108013910)

[Appendix E – Information Asset Owner Role 31](#_Toc108013911)

[Appendix F – Information Governance Steering Group Terms of Reference 32](#_Toc108013912)

[Appendix G – National Data Security Standards 33](#_Toc108013913)

[Appendix H – Data Protection Impact Assessments 34](#_Toc108013914)

[Appendix I – Contract Clauses 36](#_Toc108013915)

[Appendix J – Incident Management and Reporting 50](#_Toc108013916)

[Appendix K – Information Governance Training Needs Assessment 53](#_Toc108013917)

## Introduction

Information is a vital asset clinically and non-clinically and for the efficient management of services, resources and performance. It is therefore important that an appropriately robust policy framework is in place. IG stipulates the way in which information, and particularly in an NHS environment, Personal Confidential Data (PCD) should be handled. PCD is:

* Personal information about identifiable individuals, which should be kept private.
* The Data Protection (DP) legislation definition of personal and special categories of data, adapted to include those who have passed away (see next two paragraphs for definitions).
* Information ‘given in confidence’ and ‘that which is owed a duty of confidence’.

Under the legislation Personal Data is defined as:

Any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

And Special Categories of Personal Data is defined as:

Racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.

IG also enables the ICB to ensure that all confidential information is dealt with legally, securely and efficiently, in order to deliver the best possible care to its patients.

The aim of this framework and policy is to set out how the ICB will effectively manage IG.

This framework and policy has been developed to locally implement national legislation and guidance including, though not limited to:

* A Manual for Caldicott Guardians (2017).
* Access to Health Records Act 1990.
* Computer Misuse Act 1990.
* Common Law Duty of Confidentiality.
* CQC Safe Data, Safe Care (2016).
* Data Protection Act 2018.
* Environmental Information Regulations.
* Freedom of Information Act 2000.
* General Data Protection Regulation.
* Health Service Control of Patient Information Regulation (COPI) 2002.
* Health and Social Care Act 2012.
* Health and Social Care (Safety and Quality) Act 2015.
* Confidentiality NHS Code of Practice (2003).
* Human Rights Act 1998.
* Records Management Code of Practice for Health and Social Care (2016).
* Information Security Management Code of Practice (2007).
* Information: To Share or Not to Share (2013) (Caldicott2).
* Privacy and Electronic Communications Regulations.
* Report on the Review of Patient-Identifiable Information (1997) (The Caldicott Report).
* Review of Data Security, Consent and Opt-Outs (2016) (Caldicott 3).

Any action taken to comply with Information Governance guidance will not amount to discrimination because of protected characteristics as set out in the Equality Act 2010.

## Purpose / Policy Statement

This framework and policy sets out the IG agenda for the ICB.

This framework and policy is based on Department of Health (DH) guidelines and Data Protection (DP) related law. The main piece of legislation being the Data Protection Act 2018 (DPA), which includes the UK version of the European Union General Data Protection Regulation 2016 (GDPR).

The GDPR has six principles, that Personal Confidential Data (PCD) must be processed:

* Fairly, lawfully and transparently.
* For specified purposes.
* Using the minimum amount necessary.
* Accurately.
* For only as long as it is needed.
* Securely.

Furthermore, Data Subjects have increased rights to:

* Information about how their information is being processed.
* Access to their information.
* Rectification when information is wrong.
* Be forgotten; when it is appropriate to do so.
* Restrict processing.
* Data portability.
* Object to processing.
* Appropriate decision making.

In health and social care the Caldicott Principles reflect these, by stating that when using PCD, staff must observe the following:

* Justify the purpose(s).
* Don’t use it unless it is absolutely necessary.
* Use the minimum necessary.
* Access should be on a strict need to know basis.
* Everyone with access to it should be aware of their responsibilities.
* Comply with the law.
* The duty to share information can be as important as the duty to protect patient confidentiality.
* Inform patients and service users about how their confidential information is used.

## Definitions

The following abbreviations and acronyms are used throughout this document, definitions are provided within the content of the document.

* AGEM Arden & Gem CSU.
* AO Accountable Officer.
* BC Business Continuity.
* CG Caldicott Guardian.
* CIO Chief Information Officer.
* COPI Control of Patient Information Regulation 2002.
* DFM Data Flow Mapping.
* DH Department of Health.
* DP Data Protection.
* DPA Data Protection Act 2018.
* DPIA Data Protection Impact Assessment.
* DPO Data Protection Officer.
* DSPT Data Security and Protection Toolkit.
* EIR Environmental Information Regulations 2004.
* ESR Electronic Staff Record.
* EU European Union.
* FOIA Freedom of Information Act 2000.
* GDPR General Data Protection Regulation.
* IA Information Asset.
* IAA Information Asset Administrator.
* IAM Information Asset Management.
* IAO Information Asset Owner.
* IAR Information Asset Register.
* ICB Integrated Care Board.
* ICO Information Commissioner’s Office.
* ICS Integrated Care System.
* IG Information Governance.
* IGSG Information Governance Steering Group.
* InfoSec Information Security.
* IRM Information Risk Management.
* ISA Information Sharing Agreement.
* NHSD NHS Digital.
* PCD Personal Confidential Data.
* PIA Privacy Impact Assessment.
* PID Person Identifiable Data.
* SAR Subject Access Request.
* SIC Statement of Internal Control.
* SIRI Serious Incident Requiring Investigation.
* SIRO Senior Information Risk Owner.
* TNA Training Needs Analysis.

## Roles and Responsibilities

### All ICB Employees and Board members

* + 1. Many staff handle information in one form or another. Staff who in the course of their work create, use, or otherwise process information have a duty to keep up to date with and adhere to, relevant legislation, case law and national guidance.
		2. The ICB policies and procedures will reflect such guidance and compliance with these polices and will ensure a high standard of Information Governance compliance within the organisation.
		3. All staff and officers, whether permanent, temporary, contracted or contractors are responsible for ensuring that they are aware of their responsibilities in respect of Information Governance.

### Integrated Care Board

* + 1. Has ultimate responsibility and accountability for ensure that the organisation corporately meets its legal responsibilities and for the adoption of internal and external governance requirements.

### Chief Executive

* + 1. Has overall responsibility for information governance within the ICB. The AO is responsible for the management of Information Governance and for ensuring appropriate mechanisms are in place to support service delivery and continuity.

### Senior Information Risk Owner (SIRO)

* + 1. The role of Senior Information Risk Owner (SIRO) in the ICB has been assigned to the Director of Resources.
		2. The SIRO is responsible for leading on Information Risk and for overseeing the development of an Information Risk Policy.
		3. The SIRO is also responsible for ensuring the corporate risk management process includes all aspects of information risk and for guaranteeing the ICB Board is adequately briefed on information risk issues.
		4. See Appendix B for a more detailed description of the SIROs role and responsibilities.

### Caldicott Guardian

* + 1. The role of Caldicott Guardian in the ICB has been assigned to the Executive Chief Nursing Officer.
		2. The Caldicott Guardian has particular responsibilities for protecting the confidentiality of patients/service-user’s information and enabling appropriate information sharing.
		3. Acting as the 'conscience' of the organisation, the Caldicott Guardian will actively support work to enable information sharing where it is appropriate to share and will advise on options for lawful and ethical processing of information.
		4. See Appendix C for a more detailed description of the Caldicott’s role and responsibilities.

### Head of Information Governance / Data Protection Officer (DPO)

* + 1. The Head of Information Governance has the leadership function for IG, maintaining the confidence of patients, staff and the public, through advice and guidance on the creation of robust and effective mechanisms and assurance processes to protect and appropriately handle PCD.
		2. This includes ensuring that the ICB is fully compliant with all IG related legislation and that the ICB meets statutory and mandatory obligations for IG through development of strategy and implementation of IG policies.
		3. The Head of Information Governance is also the ICB’s Data Protection Officer.
		4. See Appendix D for a more detailed description of the DPO’s role and responsibilities.

### Information Governance Team

* + 1. The team acts under the guidance of the Head of IG to provide support and guidance on all Information Governance related issues to staff and GP practices across Essex.

### Associate Director of IT

* + 1. Ins The role of the Head of Information Governance is supported by the Associate Director of IT & AGEM CSU.
		2. They are responsible for:
* Developing, implementing and enforcing suitable and relevant information security procedures and protocols to ensure the ICB’s systems and infrastructure remain compliant with data protection legislation, and for ensuring that all the ICB’s electronic equipment and assets have adequate security measures to comply with data protection and data security legislation and regulations.
* Acting as the Information Asset Owner for the IT infrastructure with specific accountability for computer and telephone equipment and services that are operated by corporate and clinical work force, e.g., personal computers, laptops, personal digital assistants and related computing devices, held as an NHS asset.
* Work with the Information Governance team and DPO as appropriate regarding matters relating to data and IT security.

### Information Security Officer

* + 1. Technical information security issues, operational and strategic authority rests with the IT Service Provider – Arden & Greater East Midlands Commissioning Support Unity (AGEM CSU).
		2. AGEM will have a nominated Information Security Officer / Manager with appropriate duties and resources.
		3. AGEM will provide support to the ICB in ensuring compliance to the relevant sections of the Data Security & Protection Toolkit (DSPT) as well as Data Protection Legislation and national guidance, as set out within their contract.

### Information Asset Owners (IAOs)

* + 1. Designated Information Asset Owners (IAOs) are senior members of staff at director / assistant director level or heads of department responsible for providing assurance to the SIRO that information risks, within their respective areas of responsibility are identified and recorded and that controls are in place to mitigate those risks.
		2. See Appendix E for a more detailed description of an IOA’s roles and responsibilities.

### Information Asset Administrators (IAAs)

* + 1. Information Asset Owners can appoint Information Asset Administrators (IAAs) to support in the delivery of their information risk management responsibilities.
		2. Information Asset Administrators ensure that policies and procedures are followed, recognise actual or potential security incidents and take steps to mitigate those risks, consult with their Information Asset Owner on incident management and ensure that information asset registers are accurate and up to date.

### Information Governance Steering Group (IGSG)

* + 1. The IGSG is responsible for overseeing the implementation of the Information Governance Policy and Management Framework and the annual IG assessment.
		2. The group also reviews and approves IG related documentation.
		3. The Group reports into the Audit Committee.
		4. See Appendix F for the Terms of Reference for the IGSG.

## Policy Detail

### Overarching Legislation and Principles

* + 1. A range of components fall under IG as it overlaps with clinical governance and is a subset of corporate governance. The overarching NHS framework is outlined in the Data Security and Protection Toolkit (DSPT). Known as the National Data Security Standards, they are drawn from the 2016 Caldicott 3 Report and are outlined in Appendix G.
		2. In its management of PCD, the ICB complies with DP and Caldicott Principles. Under the law, PCD must be processed in line with six principles:
* Fairly, lawfully and transparently.
* For specified purposes.
* Using the minimum amount necessary.
* Accurately.
* For only as long as it is needed.
* Securely.
	+ 1. Data Subjects also have rights under the legislation to:
* Information about how their information is being processed. The ICB addresses this by ensuring a layered approach to informing data subjects how their information is used, including posters, pamphlets and service level leaflets.
* Access to their information. Data Subjects may request access to personal information that the ICB holds about them. This type of request is known as a Subject Access Request.
* Rectification when information is wrong. Any request for rectification will be assessed on a case-by-case basis using the precedent of the ICB’s developing experience of the legislation, along with relevant case law.
* Be forgotten (when it is appropriate). In healthcare information needs to be retained for care and medico-legal purposes, rendering this right largely exempt. Any request to be forgotten will be assessed on a case-by-case basis using the precedent of the ICB’s developing experience of the legislation, along with relevant case law.
* Restrict processing. Data Subjects may request that the ICB hold only sufficient Personal Data about them, but not process it any further. Any request for restriction of processing will be assessed on a case-by-case basis using the precedent of the ICB’s developing experience of the legislation, along with relevant case law.
* Data portability. This allows Data Subjects to obtain and reuse their information across different services. In healthcare there are not expected to be many requests, as much information is available as a Subject Access Request (SAR). Any request for portability of data will be assessed on a case by case basis using the precedent of the ICB’s developing experience of the legislation, along with relevant case law.
* Object to processing. This allows the Data Subject to object if they do not believe the use of their information is legitimate. Any request to object will be assessed on a case by case basis using the precedent of the ICB’s developing experience of the legislation, along with relevant case law.
* Appropriate decision making. The ICB is required to demonstrate that it has a lawful basis to carry out profiling and / or automated decision making.
	+ 1. All requests from Data Subjects to exercise their rights must normally be responded to within 30 days, unless there are extenuating circumstances, in which case there are some rights to extension under the legislation. The full text of the DPA is on the Government’s legislation website.
		2. In the NHS, the Caldicott Principles are equally as important when using PCD to:
* Justify the purpose(s).
* Not use it unless it is absolutely necessary.
* Use the minimum necessary.
* Ensure access is on a strict need to know basis.
* Ensure everyone with access to it is aware of their responsibilities.
* Comply with the law.
* The duty to share information can be as important as the duty to protect patient confidentiality.
* Information patients and service users about how their confidential information is used.
	+ 1. Full detail about Caldicott is in Information: To Share or Not to Share (2013).
		2. The ICB also ensures compliance with the Freedom of Information Act 2000 (FOIA) and the associated Lord Chancellor’s Codes of Practice under sections 45 and 46. This is set out in the ICB’s Access to Information Policy.

### Annual Information Governance Audit

* + 1. The ICB has an annual audit of its Data Security & Protection Toolkit compliance by its internal auditors.

###  Mandatory Training and Awareness

* + 1. Fundamental to the success of delivering a robust IG agenda across the ICB is the development of an IG aware culture. Training is provided both online and face to face to all staff to promote this ethos. In practical terms, this means 95% of all staff (which includes staff not available to complete the training, such as staff on long term sick leave, maternity leave and so on) must be trained.
		2. In addition to formal IG training, the ICB has an IG Resource Guide that is supplied to all staff together with ad-hoc updates across the year.
		3. Some roles, such as SIRO, Caldicott Guardian, IAOs and those with access to PCD are required to undertake additional training to remain current in their role.
		4. All decisions on the need for training will be documented in a Training Needs Analysis, which must be ratified by IGSG (included as appendix K).

### Confidentiality Code of Conduct

* + 1. All staff must be aware of their individual responsibilities for the maintenance of confidentiality, DP, Information Security (InfoSec) management and data quality. They are given the tools for this through undertaking annual mandatory IG training and via the IG Resource Guide.

### Information Asset Management and Business Continuity

* + 1. A core IG objective is that information assets (IAs) and the use of information contained within are identified and that the business importance of those assets is established.
		2. IAs are those that are central to the efficient running of the ICB and specific departments, for example, clinical systems (such as Broadcare), record repositories (such as Datix), Oracle and so on. They also include, but are not limited to the following examples:
* Information – system documentation and procedures, archive media and data.
* Software – databases, application programs, systems, development tools and utilities.
* Physical – infrastructure, equipment, furniture, and accommodation used for data processing.
* Services – computing and communications, heating, lighting, power, air conditioning used for data processing.
* People – qualifications, skills, and experience in the use of information systems.
* Intangible – the ICB’s reputation.
	+ 1. Essentially, it is information in any format that is of value to the organisation and would be problematic if it were not accessible.
		2. The ICB has clear lines of accountability for Information Risk Management (IRM) that lead directly to the Board through the SIRO. IAOs are usually senior members of staff who are the nominated owner for one or more of the ICB’s identified information assets (see Appendix 4) and report for this function to the SIRO.
		3. Within their area of responsibility, it is the IAOs role to log the IAs held and to ensure this is documented in an Information Asset Register (IAR) and undertake a Data Flow Mapping (DFM) exercise. Collectively these Information Asset Management (IAM) activities are owned by the IAOs, who are accountable for their effective completion.
		4. Whereas it is ideal that all assets are clearly identified on the IAR, the ICB has a risk-based approach that gives priority to IAs that comprise or contain PCD and / or would have the greatest impact on patients, staff, a particular department and / or the ICB if they were not available.
		5. The SIRO has the final decision on approving identified risk mitigation plans. Serious risks must be entered onto the Corporate Risk Register for Board consideration.
		6. IAOs are mandated by the SIRO to receive training, delivered by the IG Team, to ensure they remain effective in their role.
		7. Data in the IAR includes necessary information to assist in a business continuity (BC) event. IAOs must ensure that IAM risk assessments are performed at least annually and that any significant risks to their asset, whether identified in the annual risk assessment or on an ad hoc basis, are reported immediately to the SIRO.
		8. All information and assets associated with information processing facilities must be owned by a designated part of the organisation. The IAO is responsible for ensuring that information and assets associated with information processing facilities are appropriately identified and classified, defining and reviewing access restrictions, classifications and BC arrangements taking into account applicable access control policies.
		9. All changes to IA, such as system upgrades, should follow an established change control procedure, such as a DPIA.
		10. IAOs are encouraged, as best practice, to engage an IA Administrator to support them in their role, to ensure that policies and procedures are followed, recognise actual or potential security incidents, consult their IAO on incident management and ensure that records are accurate and up to date.
		11. When considering transferring PCD outside of the European Union (EU) it is important under the new legislation to ensure there is a legitimate basis for doing so when those jurisdictions do not have adequate DP regulation, as this ensures Data Subjects information is not undermined. Whereas this changes little from previously, there is now greater encouragement to use transfer adequacy Codes of Practice and Certification Schemes.

### Information Risk Management

* + 1. The ICB is committed to making the best use of the information it holds to provide efficient healthcare and services to its patients and the local health economy while ensuring that adequate safeguards are in place to keep information secure and to protect Data Subjects right to privacy.
		2. The ICB recognises that information handling represents a significant corporate risk in that failures to protect information properly or use it appropriately can have a damaging impact on its reputation. Furthermore, failure to protect information adequately can attract the attention of the Information Commissioner’s Office (ICO), which regulates DP and has access to a range of sanctions including significant fines.
		3. IRM complements the ICB’s risk management framework. As part of this, information risks are clearly recognised and the appropriate controls implemented through a Board approved corporate risk management strategy and policy.
		4. Information risk is intrinsic in all administrative and business activities and all staff must continuously manage it. The ICB recognises that the aim of IRM is not to eliminate risk, but to provide the structural means to manage it, by balancing its treatments with anticipated benefits that maybe derived.
		5. The ICB acknowledges that IRM is an essential element of broader IG and InfoSec arrangements and is an integral part of good management practice; it should not be seen as an additional requirement.
		6. The risk management framework is dependent on allocating clear organisational responsibilities, identifying all the IAs, assessing the associated risks and managing any incidents arising from them. This will:
* Protect the ICB, its staff and its patients from information risks where the likelihood of occurrence and the impact is significant.
* Provide a consistent risk management framework in which information risks will be identified, considered and addressed.
* Encourage proactive rather than reactive risk management.
* Inform decision making throughout the ICB.
* Meet legal and statutory requirements.
* Assist in safeguarding the ICB’s IAs.
	+ 1. Information Risk Assessments are performed for all information systems and critical IAs at the following times:
* At least annually, as an integral part of the IAM process.
* Ahead of introducing new systems, applications, facilities and so on that may impact the assurance of ICB information or systems, using a DPIA.
* Ahead of agreeing enhancements, upgrades and conversions associated with critical systems or applications. Those containing or which involve personal information will also require a DPIA.
* When NHS policy, legislation or associated guidance requires risk determination, or when that legislation and guidance is changed or updated.
* When required by the ICB, as directed by the SIRO, Caldicott Guardian or Head of Information Governance / Data Protection Officer.
	+ 1. As in the ICB’s overarching Risk Management Policy, any risk assessments scoring high or above must be entered onto the Corporate Risk Register. For those undertaken as part of the IAM process, every attempt is taken to treat, mitigate or eliminate risks scored as anything other than green on the red/amber/yellow/green scoring matrix. Any scoring red will be considered by the SIRO for addition to the Corporate Risk Register. The DPIA process is intentionally designed to ensure all new / amended processes are introduced with the least possible risk apparent.
		2. Information incident reporting is in line with the ICB‘s overall incident reporting processes. Additional guidance is drawn from NHS Digital’s (NHSD) Guide to the Notification of Data Security and Protection Incidents.
		3. Indicators that IRM is being positively enacted include, but are not limited to, successful completion of the DSPT and there having been no involvement from the ICO as a result of significant DP breaches.
		4. An annual review will be carried out by the IG Team on behalf of the SIRO. Overall responsibility for action plans lies with the SIRO, to be completed by relevant IAO.

### Records of Processing Activities

* + 1. The Information Asset Registers and Data Flow Mapping spreadsheets also act as the ICB’s Records of Processing Activities as required under GDPR.
		2. These detail the purposes of processing, categories of data subjects, categories of personal data, recipients of personal data, any transfers to a third country, time limits for erasure, security measures in place to protect the data and the legal basis for processing the data.

### Data Protection Impact Assessments (DPIA)

* + 1. In line with ICOs guidance, a DPIA must be undertaken for any project, procurement, business case, use of or transfer of personal data or departmental / team initiative where there is a potential impact upon the privacy of individuals.
		2. DPIAs are a risk assessment tool to analyse how a particular project or system will affect the privacy of the individuals involved. Projects are not formally defined by the ICB but are considered to be any plan or proposal (potential, proposed or realised), procurement, business case or departmental / team initiative that include the use of or transfers of Personal Data.
		3. The DPIA process must be integral to conventional project management techniques and be started from the very earliest stages of the project’s initiation.
		4. DPIAs are chiefly concerned with an individual’s ability to manage their information; the ICB’s processes are therefore aligned to DP and Caldicott principles, with specific concentration being given to the minimising of harm arising from intrusion into privacy, as defined by those principles.
		5. An effective DPIA allows the organisation to identify and resolve any such problems at an early stage, minimising costs and reputational damage which might otherwise occur.
		6. For further procedural detail see Appendix H.

### InfoSec, Cyber Security and User Access Controls

* + 1. ISO 270001, the International Standard on Information Security defines the concept as the ‘Preservation of confidentiality, integrity and availability of information’, adding that other properties are involved, such as authenticity, accountability, non-repudiation, and reliability.
		2. Increasingly all organisations and their information systems and networks are faced with security threats from a wide range of sources, including lost or stolen equipment or data, computer assisted fraud, sabotage, vandalism, fire, or flood.
		3. The ICB ensures that PCD is protected by encryption in accordance with DH directives.
		4. To prevent unauthorised access to information systems, formal procedures are in place to control the allocation of access rights to information systems and services, which cover all stages in the lifecycle of system access.
		5. Users are made aware of their responsibilities for maintaining effective access controls through the inclusion of InfoSec in IG training, particularly regarding the use of passwords and the security of equipment.
		6. Security facilities at the operating system level should be used to restrict access to computer resources, including terminal identification, access records, authentication mechanisms and access time restrictions.
		7. Cyber and InfoSec are managed by AGEM CSU on behalf of the ICB.

### Safe Haven

* + 1. All transfers of PCD, for whatever reasons, must wherever possible, be undertaken within a safe haven environment, to ensure it adheres to the legal restrictions that govern transfer of such information.
		2. The term “Safe Haven” is recognised throughout the NHS to describe the administrative arrangements and physical measures that must be implemented to safeguard the confidential transfer of PCD between organisations or sites using any of the following formats or methods:
* Fax Machines.
* Post / E-mail.
* Telephones / Answer Phones.
* Computer Systems / Electronic Media.
* Manual Records.
* White Boards / Notice Boards.
	+ 1. Detailed operational guidance, which must be followed, is available for staff within the Information Governance Resource Guide.

### Records Management

* + 1. The ICB is committed to a systematic and planned approach to the management of records within the organisation, from their creation to their ultimate disposition.
		2. The ICB ensures it controls the quality and quantity of the information that it generates, can maintain that information in an effective manner and can dispose of the information efficiently and securely when it is no longer required.
		3. Records are managed in accordance with the Records Management Code of Practice for Health and Social Care, as set out in the Records Management & Lifecycle Management Policy.

### Contracts

* + 1. The ICB uses the NHS Standard Contract for most of its contracting, which includes clauses relating to IG. Where the NHS Standard Contract is not used, a set of standard contract clauses have been developed (See Appendix I).
		2. It is the joint responsibility of the Commissioning / Procurement Team and the owning manager of the contract to ensure the contract is IG compliant.
		3. The SIRO and IAOs must take all reasonable steps to ensure that contractors and support organisations to whom PCD is disclosed comply with their contractual obligations to keep PCD secure and confidential.
		4. Directors, managers at all levels and IAOs must ensure that all existing contracts are monitored and reviewed annually to ensure that IG controls are being adhered to and to resolve problems or unforeseen events.
		5. An accurate register of all contracts must be maintained by the ICB and is managed by the contracts team.

### Processing Data, the Use of Consent, and Information Sharing

* + 1. Sharing and use of information about an individual within the organisation and between partner agencies is vital to the provision of coordinated and seamless provision of care and services. The ICB keenly recognises the need for shared information and robust InfoSec to support the implementation of joint working arrangements. The uses and sharing of clinical data can be divided into two broad categories.
		2. The first of these is immediate Direct Care, which the Independent IG Oversight panel defines as:

*A clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. It includes supporting individuals’ ability to function and improve their participation in life and society. It includes the assurance of safe and high-quality care and treatment through local audit, the management of untoward or adverse incidents, person satisfaction including measurement of outcomes undertaken by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their care.*

* + 1. For such use patient consent is not generally required under the UK’s data protection legislation. However, practitioners must maintain an awareness of the Common Law Duty of Confidentiality, that if the patient disclosed information in circumstances where it was expected that a duty of confidence applied, it should not normally be further disclosed without that Data Subject’s consent. If this has not been obtained it is beholden on the member of staff intending to share personal information to make an appropriate decision based on whether disclosure is essential to safeguard either the Data Subject or a third party and is considered to be in the public interest. There may also be a legal obligation to share the information, such as a Court Order.
		2. The second category is Secondary Uses, which the National IG Board defines as:

*Any purpose which does not “directly contribute to the diagnosis, care and treatment of an individual and the audit/assurance of the quality of the healthcare provided” to the individual’.*

* + 1. For such use patient consent is generally required. This is defined as ‘freely given, specific, informed and unambiguous indication of the Data Subject's agreement to the processing of Personal Data relating to him or her, such as by a written statement, including by electronic means, or an oral statement’.
		2. However, under UK DP legislation consent is not required where there is another condition for processing. There are specific legal gateways for sharing PCD for the planning of services and management of health and social care systems and services. For such uses a DPIA must be completed where identifiable Special Categories of Data are present and formal advice must be sought from the IG Team. A documented Information Sharing Agreement (ISA) is highly likely to be required.
		3. An ISA is good practice and can be a useful way of providing transparency for organisations needing to exchange information, providing assurance in respect of the standards that each party agrees to adopt.
		4. Beyond sharing for immediate Direct Care and Secondary Uses, an ISA is required for large scale regular / permanent sharing, such as giving access to a clinical system.
		5. For use of PCD in other circumstances, the Secretary of State for Health is permitted to make regulations to set aside the Common Law Duty of Confidentiality for defined medical purposes under Section 251 of the National Health Service Act 2006. These are essential activities of the NHS, and important medical research, that require the use of PCD but, because patient consent had not been obtained to use it for these other purposes, there was no secure basis in law.
		6. Section 251 can be utilised when it is not possible to use anonymised information and where seeking consent is impractical, having regard to the cost and technology available. It is administered by the NHS Health Research Authority, through a Confidentiality Advisory Group.
		7. For further information on information sharing processes and templates see The ICB’s Information Sharing Policy.

### Data Quality Assurance

* + 1. The quality of information acquired and used within the ICB is a key component to its effective use and management.
		2. As such, IAOs and managers are expected to take ownership of, and seek to improve, the quality of data collected and held within their services.

### Subject Access Requests

* + 1. All living individuals, whether patients or staff, have a right to verify the lawfulness of the processing by:
* Having it confirmed to them that their data is being processed.
* Being given access to their Personal Data.
* Being given supplementary information, akin to that given in a Privacy Notice, explaining why the data is being processed.
	+ 1. The IG Team is responsible for dealing with most SARs received by the ICB. They must be processed within a statutory 30 days, using a defined Subject Access Request Procedure.
		2. Applications from third parties for access to records of deceased patients are managed by the IG Team under the provisions of the Access to Health Records Act 1990, in line with DHs Guidance for Access to Health Records Requests.
		3. Staff must be aware that anything they record about patients or colleagues, wherever it is stored, legally could and should in principle be released when a request is received, as all information technically forms part of the data subjects wider HR or medical record.
		4. For more detailed information on Subject Access Requests and how they are handled within the ICB please see the Access to Information Policy.

### Disclosure of Information to the Police

* + 1. Under the law the Police and other law enforcement agencies do not have automatic right to see PCD about patients or staff. However, the ICB will cooperate with them as much as possible when it is legal to do so.
		2. When requests are received, even with a Police Officer in attendance, each one must be considered individually on its own merit. PCD will not be released without careful consideration.
		3. Requests from the Police under the Crime and Taxation provisions of the Data Protection Act 2018 allow for the release of personal and special categories of data for ‘the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security’.
		4. The ICB requires any request to release personal or sensitive data about patients or staff to be signed or countersigned by a police officer of at least inspector rank.
		5. The types of scenarios where requests are likely to be considered appropriate are based on those outlined in the Confidentiality: NHS Code of Practice and include, but are not limited to, murder, manslaughter, rape, treason, kidnapping, child abuse, serious harm to state security, serious harm to public order, as well as crimes involving substantial financial gain.
		6. As most requests are unlikely to be urgent, they will be processed by the IG Team usually during normal office hours. In difficult cases the IG Team, along sometimes with the SIRO and / or Caldicott Guardian, will assess the decision to release to the Police.
		7. However, unless there is a legal basis to do so the ICB is not obliged to make a release and will make decisions based on a public interest test.

### Information Governance, Infosec and Cyber Security Incidents

* + 1. The IG Team must be informed immediately of all IG, InfoSec and cyber security incidents. These include, but are not limited to, NHSD’s classifications:
* Lost in transit.
* Lost or stolen hardware.
* Lost or stolen paperwork.
* Disclosed in error.
* Uploaded to website in error.
* Non-secure disposal – hardware.
* Non-secure disposal – paperwork.
* Technical security failing (including hacking).
* Unauthorised access / disclosure.
	+ 1. On receiving notification of a potential serious incident requiring investigation, the IG Team will inform the SIRO, Caldicott Guardian, and IG Champion as soon as practicably possible (if they are not already aware) to seek advice and guidance, as appropriate.
		2. The decision to report externally to the ICO is made in line with NHSD’s Guide to the Notification of Data Security and Protection Incidents, with the ultimate decision being the SIRO, based on the advice of colleagues in the previous paragraph.
		3. IGSG has a key function to monitor and review IG incident trends and guide overarching remedial action to those trends.
		4. See Appendix J for further details on incident management and reporting.

## Monitoring Compliance

The ICB will use a variety of methods to monitor compliance with the processes in this policy, including as a minimum the following method/s:

**IG Incidents** - Information Governance compliance will be monitored quarterly through the monitoring of reported IG incidents by the IG Steering Group.

The IG Steering Group has responsibility for providing assurances that this policy is adequate for providing clear guidance in the event of significant changes which may affect it. The IG Lead will ensure that adequate arrangements exist for:

* Reporting incidents and Caldicott issues
* Analysing and upward reporting of incidents and adverse events
* Reporting IG work programs and progress reports
* Reporting Data Security & Protection Toolkit assessments and improvement plans
* Communicating IG developments.

**Privacy Impact Assessments** - Risks will be identified and monitored through the Privacy Impact Assessment process for all new and / or changed processes, systems and / or services.

In addition to the monitoring arrangements described above, the ICB may undertake additional monitoring of this framework as a response to the identification of any gaps, or because of the identification of risks arising from the framework prompted by incident review, external reviews or other sources of information and advice.

## Staff Training

See Appendix K for IG Training Needs Assessment.

## Arrangements for Review

This policy will be reviewed no less frequently than every two years. An earlier review will be carried out in the event of any relevant changes in legislation, national or local policy/guidance, organisational change or other circumstances which mean the policy needs to be reviewed.

If only minor changes are required, the sponsoring Committee has authority to make these changes without referral to the Integrated Care Board. If more significant or substantial changes are required, the policy will need to be ratified by the relevant committee before final approval by the Integrated Care Board.

## Associated Policies, Guidance and Documents

The following documentation relates to the management of information and together underpins the ICB’s Information Governance Assurance Framework. This policy should be read in conjunction with other policies:

* Information & Cyber Security Policy.
* Records Management & Lifecycle Policy.
* Information Sharing Policy.
* Access to Information Policy.

## Equality Impact Assessment

The EIA has identified no equality issues with this policy.

The EIA has been included as Appendix A.

## Appendix A - Equality Impact Assessment

#### Assessor’s Name: Iain Gear

#### Assessor’s Job Title: Information Governance Lead

#### Date: 15th June 2022

#### Outcomes

Briefly describe the aim of the policy and state the intended outcomes for staff.

The Information Governance Framework and Policy will support the organisation and its staff to achieve legislative requirements in relation to the effective management and governance of personal information.

#### Evidence

What data/information have you used to assess how this policy might impact on protected groups?

The ICB regularly monitors the make-up of the workforce and patient population, including protected groups.

Who have you consulted with to assess possible impact on protected groups? If you have not consulted other people, please explain why?

Mid and South Essex Information Governance Steering Group; MSE Audit Committees meeting in common

#### Analysis of impact on equality

The Public Sector Equality Duty requires us to **eliminate** discrimination, **advance** equality of opportunity and **foster** good relations with protected groups. Consider how this policy / service will achieve these aims.

N.B. In some cases it is legal to treat people differently (objective justification).

* **Positive outcome** – the policy/service eliminates discrimination, advances equality of opportunity and fosters good relations with protected groups.
* **Negative outcome** – protected group(s) could be disadvantaged or discriminated against.
* **Neutral outcome** – there is no effect currently on protected groups.

Consider direct and indirect discrimination, harassment and victimisation.

| ProtectedGroup | Positiveoutcome | Negativeoutcome | Neutraloutcome | Reason(s) for outcome |
| --- | --- | --- | --- | --- |
| Age |  |  | X | The policy refers to ensuring that “Any action taken to comply with Information Governance guidance will not amount to discrimination because of protected characteristics as set out in the Equality Act 2010.” |
| Disability(Physical and Mental/Learning) |  |  | X | As above |
| Religion or belief |  |  | X | As above |
| Sex (Gender) |  |  | X | As above |
| Sexual Orientation |  |  | X | As above |
| Transgender/Gender Reassignment |  |  | X | As above |
| Race and ethnicity |  |  | X | As above |
| Pregnancy and maternity (including breastfeeding mothers) |  |  | X | As above |
| Marriage or Civil Partnership |  |  | X | As above |

#### Monitoring Outcomes

Monitoring is an ongoing process to check outcomes. It is different from a formal review which takes place at pre-agreed intervals.

What methods will you use to monitor outcomes on protected groups?

#### The ICB undertakes regular monitoring and gap analysis through the Information Asset Registers, Data Protection Impact Assessments and IG related incident investigations.

#### Review

How often will you review this policy / service?
(Minimum every three years).

Every two years.

## Appendix B – Senior Information Risk Owner Role

The Senior Information Risk Owner (SIRO) should be an Executive Director or other senior member of the Board (or equivalent senior management group/committee). The SIRO may also be the Chief Information Officer (CIO) if the latter is on the Board but should not be the Caldicott Guardian as the SIRO should be part of the organisation's management hierarchy rather than being in an advisory role.

The SIRO will be expected to understand how the strategic business goals of the organisation may be impacted by information risks and it may therefore be logical for this role to be assigned to a Board member already leading on risk management or information governance.

The SIRO will act as an advocate for information risk on the Board and in internal discussions and will provide written advice to the Accounting Officer on the content of the annual Statement of Internal Control (SIC) in regard to information risk, provide an essential role in ensuring that identified information security risks are followed up and incidents managed and should have ownership of the Information Risk Policy and associated risk management Strategy and processes. They will provide leadership and guidance to Information Asset Owners.

The key responsibilities of the SIRO are to:

* Oversee the development of an Information Risk Policy, and a Strategy for implementing the policy within the existing Information Governance Framework.
* Take ownership of the risk assessment process for information and cyber security risk, including review of an annual information risk assessment to support and inform the Statement of Internal Control.
* Review and agree action in respect of identified information risks.
* Ensure that the organisation’s approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff.
* Provide a focal point for the resolution and/or discussion of information risk issues.
* Ensure the Board is adequately briefed on information risk issues.
* Ensure that all care systems information assets have an assigned Information Asset Owner.
* Oversee the formulation and implementation of IT related policies and the creation of supporting procedures, ensuring these are embedded within the service and developing, implementing and managing robust IT security arrangements in line with best industry practice.
* Oversee effective management and security of the ICB’s IT resources, for example, infrastructure and equipment.
* Oversee development and implementation of a robust IT Disaster Recovery Plan;
* Ensuring that IT security levels required by the NHS Statement of Compliance are met.
* Ensuring the maintenance of all firewalls and secure access servers are in place at all times.

## Appendix C – Caldicott Guardian Role

A Caldicott Guardian is a senior person within a health or social care organisation who makes sure that the personal information about those who use its services is used legally, ethically, and appropriately, and that confidentiality is maintained. Caldicott Guardians should be able to provide leadership and informed guidance on complex matters involving confidentiality and information sharing.

The Caldicott Guardian should play a key role in ensuring that their organisation satisfies the highest practical standards for handling person-identifiable information. Their main concern is information relating to patients, service users and their care, but the need for confidentiality extends to other individuals, including their relatives, staff, and others. Organisations typically store, manage, and share personal information relating to staff, and the same standards should be applied to this as to the confidentiality of patient information.

Caldicott Guardians should apply the seven principles wisely, using common sense and an understanding of the law. They should also be compassionate, recognising that their decisions will affect real people — some of whom they may never meet. The importance of the Caldicott Guardian acting as “the conscience of the organisation” remains central to trusting the impartiality and independence of their advice.

## Appendix D – Data Protection Officer Role

The Data Protection Officer reports directly to the (most senior level of management), in matters relating to data protection assurance and compliance.

**Responsibilities:**

* To provide support, advice and assurance of compliance across the ICBs.
* To maintain expert knowledge of data protection law and practices and how they apply to the business of the ICBs.
* To be the first point of contact within the ICBs for all data protection matters.
* To support programmes of work from inception to ensure that data protection is addressed by default and in design of new systems and information processes.
* Data protection officer to be published on ICBs Privacy Notice.
* The data protection officer will ensure that appropriate confidentiality is maintained in the performance of his tasks.
* In performing their tasks as the data protection officer they must ensure that the DPO responsibilities are not influenced in any way, and should a potential conflict of interest arise report it to the Chief Corporate Services Officer.
* To develop or advise senior management on the development and establishment of policies, procedures and other measures to ensure compliance with the GDPR, Data Protection Act, including but not limited to:
	+ Records of processing activities.
	+ Data protection by design and default.
	+ Data Protection Impact Assessments.
	+ Fair Processing.
* To monitor compliance with these measures and provide reports to the (most senior level of management ) tbc / Committees.
* To support programmes and initiatives that involve the development of new or innovative information processes on the need for a data protection impact assessment (DPIA).
* To support and advise programmes and initiatives in conducting data protection impact assessments, and to assure the proposed mitigations.
* To consult with the Information Commissioners Office (ICO) where proposed processing poses a high risk in the absence of proposed mitigations.
* To take account of the risks associated with processing in the performance of his tasks.
* Provision of specialist advice to the ICBs on compliance obligations.
* Provision of advice to projects and business change initiatives on when a data protection impact assessment is required.
* The DPO has final sign-off of data protection impact assessments once taken through IG Team and approved by either Caldicott / SIRO.
* To be the first point of contact for the Information Commissioners Office (ICO).
* To co-operate with the ICO in any matters relating to data protection compliance including provision of evidence of compliance, and relation to breach management.
* The DPO operates independently and is not dismissed or penalised for performing their task.

## Appendix E – Information Asset Owner Role

For information risk, IAOs are directly accountable to the SIRO and will provide assurance that information risk is being managed effectively for their assigned information assets. In large organisations IAOs will be assisted in their roles by staff acting as Information Asset Administrators (or persons with equivalent responsibilities) who have day to day responsibility for management of information risks affecting one or more assets.

It is particularly important that each IAO (or equivalent) should be aware of what information is held and the nature of and justification for information flows to and from the assets for which they are responsible.

The role of the IAO is to understand what information is held, what is added and what is removed, how information is moved, who has access and why. As a result they should be able to understand and address risks to the information and to ensure that information is fully used within the law for the public good. The IAO will also be responsible for providing or informing regular written reports to the SIRO (or equivalent), a minimum of annually on the assurance and usage of their asset.

It is important that “ownership” of Information Assets is linked to a post, rather than a named individual, to ensure that responsibilities for the asset are passed on, should the individual leave the organisation or change jobs within it.

It is the responsibility of Information Asset Owners to ensure there is good understanding of the hardware and software composition of their assigned assets to ensure their continuing operational effectiveness. This includes establishing and maintaining asset records that will help predict when asset configuration changes may be necessary.

## Appendix F – Information Governance Steering Group Terms of Reference

*To be developed following appointment of ICB SIRO in August*

## Appendix G – National Data Security Standards

The National Data Security Standards are from the National Data Guardian’s Review of Data Security, Consent and Opt-Outs (2016) (Caldicott 3) and form the structural basis of the Data Security and Protection Toolkit.

|  |
| --- |
| **Leadership Obligation 1** – People: Ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles. |
| 1. All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.
 |
| 1. All staff understand their responsibilities under the National Data Guardian’s Data Security Standards including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.
 |
| 1. All staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Toolkit.
 |
| **Leadership Obligation 2** – Process: Ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses. |
| 1. Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.
 |
| 1. Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.
 |
| 1. Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.
 |
| 1. A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.
 |
| **Leadership Obligation 3** – Technology: Ensure technology is secure and up-to-date. |
| 1. No unsupported operating systems, software or internet browsers are used within the IT estate.
 |
| 1. A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.
 |
| 1. IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian’s Data Security Standard.
 |

## Appendix H – Data Protection Impact Assessments

This guidance explains the principles, which form the basis for a Data Protection Impact Assessment (DPIA), and sets out the basic steps, which all staff should understand and must follow during the initiation phase or early assessment for the development and implementation of projects (i.e. systems, services, changes to processes or procedures etc.) at the ICB.

A DPIA must be seen as a separate process from compliance checking or data protection audit processes and is a requirement of the Data Security and Protection Toolkit ‘formerly’ known as Information Governance (IG) Toolkit, which will help the ICB comply with the obligations under other relevant legislation and regulations.

It is based on current legal requirements and professional best practice.

All staff, the IG Team members, Data Protection Officer (DPO), Senior Information Risk Owner (SIRO), Caldicott Guardian (CG) and Information Asset Owner’s (IAO) must ensure they are familiar with the contents of this guidance, which describes the standards of conducting a Data Protection Impact Assessment (DPIA).

This document should be read in conjunction with all the relevant policies, procedures, protocols and frameworks.

All staff must recognise that a Stage 1 DPIA Questionnaire form and Stage 2 DPIA form (where applicable) must be completed and submitted to the IG Team in the following circumstances and situations:

* The use of a trial period of technology, modalities or products, which use data or information.
* The use of charitable or free technology, modalities or products, which use data or information.
* Publishing personal identifiable or sensitive information or data on the internet or in other publicly available media types.
* Procurement of technology, modalities or products, which use data or information.
* De-commissioning or disposal of technology, modalities or products, which use data or information.
* A change to existing processes or technology, modalities and products, which will significantly amend the way data or information is handled or processed.
* The implementation or development of new processes, technology, modalities or products, which involve the use of data or information.
* Collection, retrieval, obtaining, recording or holding of new data or information.

A Stage 1 DPIA Questionnaire form is designed to establish whether a further assessment is needed to ensure that there is no or little risk to an individual’s privacy. A Stage 2 DPIA form goes into more detail as to what information is being processed, for what purposes and what security measures are in place to ensure that there is either no risk to privacy, or the risks have been mitigated. In some circumstances the completion of a Stage 2 DPIA may highlight risks that cannot be mitigated. In these circumstances the organisations Caldicott and SIRO will be asked to review and either accept the risk or ask for changes to be made to the project. If a high risk is highlighted that cannot be mitigated against, then the DPIA will be referred to the ICO.

Further guidance on completion of DPIA’s and the Stage 1 and Stage 2 Questionnaires are available from the IG Team.


## Appendix I – Contract Clauses

**GC21 Patient Confidentiality, Data Protection, Freedom of Information and Transparency**

**Information Governance – General Responsibilities**

21.1 The Parties must comply with Data Protection Legislation, Data Guidance, the FOIA and the EIR, and must assist each other as necessary to enable each other to comply with these obligations.

21.2 The Provider must complete and publish an annual information governance assessment in accordance with, and comply with the mandatory requirements of, the NHS Data Security and Protection Toolkit, as applicable to the Services and the Provider’s organisation type.

21.3 The Provider must.

21.3.1 nominate an Information Governance Lead.

21.3.2 nominate a Caldicott Guardian and Senior Information Risk Owner, each of whom must be a member of the Provider’s Governing Body.

21.3.3 where required by Data Protection Legislation, nominate a Data Protection Officer.

21.3.4 ensure that the Co-ordinating Commissioner is kept informed at all times of the identities and contact details of the Information Governance Lead, Data Protection Officer, Caldicott Guardian and the Senior Information Risk Owner.

21.3.5 ensure that NHS England and NHS Digital are kept informed at all times of the identities and contact details of the Information Governance Lead, Data Protection Officer, Caldicott Guardian and the Senior Information Risk Owner via the NHS Data Security and Protection Toolkit.

21.4 The Provider must adopt and implement the National Data Guardian’s Data Security Standards and must comply with further Guidance issued by the Department of Health and Social Care, NHS England and/or NHS Digital pursuant to or in connection with those standards. The Provider must be able to demonstrate its compliance with those standards in accordance with the requirements and timescales set out in such Guidance, including requirements for enabling patient choice.

21.5 The Provider must, at least once in each Contract Year, audit its practices against quality statements regarding data sharing set out in NICE Clinical Guideline 138.

21.6 The Provider must ensure that its NHS Data Security and Protection Toolkit submission is audited in accordance with Information Governance Audit Guidance where applicable. The Provider must inform the Co-ordinating Commissioner of the results of each audit and publish the audit report both within the NHS Data Security and Protection Toolkit and on its website.

21.7 The Provider must report and publish any Data Breach and any Information Governance Breach in accordance with IG Guidance for Serious Incidents. If the Provider is required under Data Protection Legislation to notify the Information Commissioner or a Data Subject of a Personal Data Breach then as soon as reasonably practical and in any event on or before the first such notification is made the Provider must inform the Co-ordinating Commissioner of the Personal Data Breach. This GC21.7 does not require the Provider to provide the Co-ordinating Commissioner with information which identifies any individual affected by the Personal Data Breach where doing so would breach Data Protection Legislation.

**Data Protection**

21.8 The Provider must have in place a communications strategy and implementation plan to ensure that Service Users are provided with, or have made readily available to them, Privacy Notices, and to disseminate nationally-produced patient information materials. Any failure by the Provider to inform Service Users as required by Data Protection Legislation or Data Guidance about the uses of Personal Data that may take place under this Contract cannot be relied on by the Provider as evidence that such use is unlawful and therefore not contractually required.

21.9 Whether or not a Party or Sub-Contractor is a Data Controller or Data Processor will be determined in accordance with Data Protection Legislation and the ICO Guidance on Data Controllers and Data Processors and any further Data Guidance from a Regulatory or Supervisory Body. The Parties acknowledge that a Party or Sub-Contractor may act as both a Data Controller and a Data Processor. The Parties have indicated in the Particulars whether they consider the Provider to be a Data Processor on behalf of one or more of the Commissioners for the purposes of this Contract.

21.10 The Provider must ensure that all Personal Data processed by or on behalf of the Provider in the course of delivering the Services is processed in accordance with the relevant Parties’ obligations under Data Protection Legislation and Data Guidance.

21.11 In relation to Personal Data processed by the Provider in the course of delivering the Services, the Provider must publish, maintain and operate.

21.11.1 policies relating to confidentiality, data protection and information disclosures that comply with the Law, the Caldicott Principles and Good Practice.

21.11.2 policies that describe the personal responsibilities of Staff for handling Personal Data.

21.11.3 a policy that supports the Provider’s obligations under the NHS Care Records Guarantee.

21.11.4 agreed protocols to govern the sharing of Personal Data with partner organisations.

21.11.5 where appropriate, a system and a policy in relation to the recording of any telephone calls or other telehealth consultations in relation to the Services, including the retention and disposal of those recordings and apply those policies and protocols conscientiously.

21.12 Where a Commissioner requires information for the purposes of quality management of care processes, the Provider must consider whether the Commissioner’s request can be met by providing anonymised or aggregated data which does not contain Personal Data.

21.12.1 Where Personal Data must be shared in order to meet the requirements of the Commissioner, the Provider must provide such information in pseudonymised form where possible.

21.12.2 the Provider must also ensure that there is a legal basis for the sharing of Personal Data.

21.13 Notwithstanding GC21.12, the Provider must (unless it can lawfully justify non-disclosure) disclose defined or specified confidential patient information to or at the request of the Co-ordinating Commissioner where support has been provided under the Section 251 Regulations, respecting any individual Service User’s objections and complying with other conditions of the relevant approval.

**The Provider as a Data Processor**

21.14 Where the Provider, in the course of delivering the Services, acts as a Data Processor on behalf of a Commissioner, the provisions of Schedule 6F (Provider Data Processing Agreement) will apply.

**Responsibilities when engaging Sub-Contractors**

21.15 Subject always to GC12 (Assignment and Sub-Contracting), if the Provider is to engage any Sub-Contractor to deliver any part of the Services (other than as a Data Processor) and the Sub-Contractor is to access personal or confidential information or interact with Service Users, the Provider must impose on its Sub-Contractor obligations that are no less onerous than the obligations imposed on the Provider by this GC21.

21.16 Without prejudice to GC12 (Assignment and Sub-Contracting), if the Provider is to require any Sub-Contractor to act as a Data Processor on its behalf, the Provider must undertake the following.

21.16.1 Require that Sub-Contractor to provide sufficient guarantees in respect of its technical and organisational security measures governing the data processing to be carried out, and take reasonable steps to ensure compliance with those measures.

21.16.2 Carry out and and record appropriate due diligence before the Sub-Contractor processes any Personal Data in order to demonstrate compliance with Data Protection Legislation.

21.16.3 as far as practicable include in the terms of the sub-contract terms equivalent to those set out in Schedule 6F (Provider Data Processor Agreement) and in any event ensure that the Sub-Contractor is engaged under the terms of a binding written agreement requiring the Sub-Contractor to undertake the following.

21.16.3.1 Process Personal Data only in accordance with the Provider’s instructions as set out in the written agreement, including instructions regarding transfers of Personal Data outside the EU or to an international organisation unless such transfer is required by Law, in which case the Data Processor shall inform the Provider of that requirement before processing takes place, unless this is prohibited by law on the grounds of public interest.

21.16.3.2 Ensure that persons authorised to process the Personal Data on behalf of the Sub-Contractor have committed themselves to confidentiality or are under appropriate statutory obligations of confidentiality.

21.16.3.3 Comply at all times with those obligations set out at Article 32 of the GDPR and equivalent provisions implemented into Law by DPA 2018.

21.16.3.4 Impose obligations as set out in this GC21.16.3 on any Sub-processor appointed by the Sub-Contractor.

21.16.3.5 Taking into account the nature of the processing, assist the Provider by taking appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Provider’s obligation to respond to requests for exercising rights granted to individuals by Data Protection Legislation.

21.16.3.6 Assist the Provider in ensuring compliance with the obligations set out at Article 32 to 36 of the GDPR and equivalent provisions implemented into Law, taking into account the nature of processing and the information available to the Sub-Contractor.

21.16.3.7 At the choice of the Provider, delete or return all Personal Data to the Provider after the end of the provision of services relating to processing, and delete existing copies unless the Law requires storage of the Personal Data.

21.16.3.8 Create and maintain a record of all categories of data processing activities carried out under the Sub-Contract, containing the following.

21.16.3.8.1 The name and contact details of the Data Protection Officer (where required by Data Protection Legislation to have one).

21.16.3.8.2 The categories of processing carried out on behalf of the Provider.

21.16.3.8.3 Where applicable, transfers of Personal Data to a third country or an international organisation, including the identification of that third country or international organisation and, where relevant, the documentation of suitable safeguards.

21.16.3.8.4 A general description of the technical and organisation security measures taken to ensure the security and integrity of the Personal Data processed under this Contract.

21.16.3.9 Guarantee that it has technical and organisational measures in place that are sufficient to ensure that the processing complies with Data Protection Legislation and ensures that the rights of Data Subject are protected.

21.16.3.10 Allow rights of audit and inspection in respect of relevant data handling systems to the Provider or to the Co-ordinating Commissioner or to any person authorised by the Provider or by the Co-ordinating Commissioner to act on its behalf.

21.16.3.11 Impose on its own Sub-Contractors (in the event the Sub-Contractor further sub-contracts any of its obligations under the Sub-Contract) obligations that are substantially equivalent to the obligations imposed on the Sub-Contractor by this GC21.16.3.

21.17 The agreement required by GC21.16 must also set out the following.

21.17.1 The subject matter of the processing.

21.17.2 The duration of the processing.

21.17.3 The nature and purposes of the processing.

21.17.4 The type of personal data processed.

21.17.5 The categories of data subjects.

21.17.6 The plan for return and destruction of the data once processing is complete unless the Law requires that the data is preserved.

**Freedom of Information and Transparency**

21.18 The Provider acknowledges that the Commissioners are subject to the requirements of FOIA and EIR. The Provider must assist and co-operate with each Commissioner to enable it to comply with its disclosure obligations under FOIA and EIR. The Provider agrees to the following.

21.18.1 That this Contract and any other recorded information held by the Provider on a Commissioner’s behalf for the purposes of this Contract are subject to the obligations and commitments of the Commissioner under FOIA and EIR.

21.18.2 That the decision on whether any exemption under FOIA or exception under EIR applies to any information is a decision solely for the Commissioner to whom a request for information is addressed.

21.18.3 That where the Provider receives a request for information relating to the Services provided under this Contract and the Provider itself is subject to FOIA or EIR, it will liaise with the relevant Commissioner as to the contents of any response before a response to a request is issued and will promptly (and in any event within 2 Operational Days) provide a copy of the request and any response to the relevant Commissioner.

21.18.4 That where the Provider receives a request for information and the Provider is not itself subject to FOIA or as applicable EIR, it will not respond to that request (unless directed to do so by the relevant Commissioner to whom the request relates) and will promptly (and in any event within 2 Operational Days) transfer the request to the relevant Commissioner.

21.18.5 That any Commissioner, acting in accordance with the codes of practice issued and revised from time to time under both section 45 of FOIA and regulation 16 of EIR, may disclose information concerning the Provider and this Contract either without consulting with the Provider, or following consultation with the Provider and having taken its views into account.

21.18.6 To assist the Commissioners in responding to a request for information, by processing information or environmental information (as the same are defined in FOIA or Environmental Information Regulations- EIR) in accordance with a records management system that complies with all applicable records management recommendations and codes of conduct issued under section 46 of FOIA, and providing copies of all information requested by that Commissioner within 5 Operational Days of that request and without charge.

21.19 The Parties acknowledge that, except for any information which is exempt from disclosure in accordance with the provisions of FOIA, or for which an exception applies under EIR, the content of this Contract is not Confidential Information.

21.20 Notwithstanding any other term of this Contract, the Provider consents to the publication of this Contract in its entirety (including variations), subject only to the redaction of information that is exempt from disclosure in accordance with the provisions of FOIA or for which an exception applies under EIR.

21.21 In preparing a copy of this Contract for publication under GC21.20 the Commissioners may consult with the Provider to inform decision-making regarding any redactions but the final decision in relation to the redaction of information will be at the Commissioners’ absolute discretion.

21.22 The Provider must assist and cooperate with the Commissioners to enable the Commissioners to publish this Contract.

**Schedule 6F- Provider Data Processing Agreement**

*[NOTE: This Schedule applies only where the Provider is appointed to act as a Data Processor under this Contract]*

1. **SCOPE**
	1. The Co-ordinating Commissioner appoints the Provider as a Data Processor to perform the Data Processing Services.
	2. When delivering the Data Processing Services, the Provider must, in addition to its other obligations under this Contract, comply with the provisions of this Schedule 6F.
	3. This Schedule 6F applies for so long as the Provider acts as a Data Processor in connection with this Contract.
2. **DATA PROTECTION**
	1. The Parties acknowledge that for the purposes of Data Protection Legislation in relation to the Data Processing Services the Co-ordinating Commissioner is the Data Controller and the Provider is the Data Processor. The Provider must process the Processor Data only to the extent necessary to perform the Data Processing Services and only in accordance with written instructions set out in this Schedule, including instructions regarding transfers of Personal Data outside the EU or to an international organisation unless such transfer is required by Law, in which case the Provider must inform the Co-ordinating Commissioner of that requirement before processing takes place, unless this is prohibited by Law on the grounds of public interest.
	2. The Provider must notify the Co-ordinating Commissioner immediately if it considers that carrying out any of the Co-ordinating Commissioner’s instructions would infringe Data Protection Legislation
	3. The Provider must provide all reasonable assistance to the Co-ordinating Commissioner in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Co-ordinating Commissioner, include:
		1. a systematic description of the envisaged processing operations and the purpose of the processing;
		2. an assessment of the necessity and proportionality of the processing operations in relation to the Data Processing Services;
		3. an assessment of the risks to the rights and freedoms of Data Subjects;
		4. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.
	4. The Provider must, in relation to any Personal Data processed in connection with its obligations under this Schedule 6F:
		1. process that Personal Data only in accordance with Annex A, unless the Provider is required to do otherwise by Law. If it is so required the Provider must promptly notify the Co-ordinating Commissioner before processing the Personal Data unless prohibited by Law;
		2. ensure that it has in place Protective Measures, which have been reviewed and approved by the Co-ordinating Commissioner as appropriate to protect against a Data Loss Event having taken account of the:
			1. nature of the data to be protected;
			2. harm that might result from a Data Loss Event;
			3. state of technological development;
			4. cost of implementing any measures;
		3. ensure that:
			1. when delivering the Data Processing Services the Provider Staff only process Personal Data in accordance with this Schedule 6F (and in particular Annex A);
			2. it takes all reasonable steps to ensure the reliability and integrity of any Provider Staff who have access to the Personal Data and ensure that they:
				1. are aware of and comply with the Provider’s duties under this paragraph;
				2. are subject to appropriate confidentiality undertakings with the Provider and any Sub-processor;
				3. are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Co-ordinating Commissioner or as otherwise permitted by this Contract;
				4. have undergone adequate training in the use, care, protection and handling of Personal Data;
				5. are aware of and trained in the policies and procedures identified in GC21.11 (*Patient Confidentiality, Data Protection, Freedom of Information and Transparency*).
		4. not transfer Personal Data outside of the EU unless the prior written consent of the Co-ordinating Commissioner has been obtained and the following conditions are fulfilled:
			1. the Co-ordinating Commissioner or the Provider has provided appropriate safeguards in relation to the transfer as determined by the Co-ordinating Commissioner;
			2. the Data Subject has enforceable rights and effective legal remedies;
			3. the Provider complies with its obligations under Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Co-ordinating Commissioner in meeting its obligations);
			4. the Provider complies with any reasonable instructions notified to it in advance by the Co-ordinating Commissioner with respect to the processing of the Personal Data;
		5. at the written direction of the Co-ordinating Commissioner, delete or return Personal Data (and any copies of it) to the Co-ordinating Commissioner on termination of the Data Processing Services and certify to the Co-ordinating Commissioner that it has done so within five Operational Days of any such instructions being issued, unless the Provider is required by Law to retain the Personal Data;
		6. if the Provider is required by any Law or Regulatory or Supervisory Body to retain any Processor Data that it would otherwise be required to destroy under this paragraph 2.4, notify the Co-ordinating Commissioner in writing of that retention giving details of the Processor Data that it must retain and the reasons for its retention;
		7. co-operate fully with the Co-ordinating Commissioner during any handover arising from the cessation of any part of the Data Processing Services, and if the Co-ordinating Commissioner directs the Provider to migrate Processor Data to the Co-ordinating Commissioner or to a third party, provide all reasonable assistance with ensuring safe migration including ensuring the integrity of Processor Data and the nomination of a named point of contact for the Co-ordinating Commissioner.
	5. Subject to paragraph 2.6, the Provider must notify the Co-ordinating Commissioner immediately if, in relation any Personal Data processed in connection with its obligations under this Schedule 6F, it:
		1. receives a Data Subject Access Request (or purported Data Subject Access Request);
		2. receives a request to rectify, block or erase any Personal Data;
		3. receives any other request, complaint or communication relating to obligations under Data Protection Legislation owed by the Provider or any Commissioner;
		4. receives any communication from the Information Commissioner or any other Regulatory or Supervisory Body (including any communication concerned with the systems on which Personal Data is processed under this Schedule 6F);
		5. receives a request from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law;
		6. becomes aware of or reasonably suspects a Data Loss Event;
		7. becomes aware of or reasonably suspects that it has in any way caused the Co-ordinating Commissioner or other Commissioner to breach Data Protection Legislation.
	6. The Provider’s obligation to notify under paragraph 2.5 includes the provision of further information to the Co-ordinating Commissioner in phases, as details become available.
	7. The Provider must provide whatever co-operation the Co-ordinating Commissioner reasonably requires to remedy any issue notified to the Co-ordinating Commissioner under paragraphs 2.5 and 2.6 as soon as reasonably practicable.
	8. Taking into account the nature of the processing, the Provider must provide the Co-ordinating Commissioner with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 2.5 (and insofar as possible within the timescales reasonably required by the Co-ordinating Commissioner) including by promptly providing:
		1. the Co-ordinating Commissioner with full details and copies of the complaint, communication or request;
		2. such assistance as is reasonably requested by the Co-ordinating Commissioner to enable the Co-ordinating Commissioner to comply with a Data Subject Access Request within the relevant timescales set out in Data Protection Legislation;
		3. assistance as requested by the Co-ordinating Commissioner following any Data Loss Event;
		4. assistance as requested by the Co-ordinating Commissioner with respect to any request from the Information Commissioner’s Office, or any consultation by the Co-ordinating Commissioner with the Information Commissioner's Office.
	9. Without prejudice to the generality of GC15 *(Governance, Transaction Records and Audit),* the Provider must allow for audits of its delivery of the Data Processing Services by the Co-ordinating Commissioner or the Co-ordinating Commissioner’s designated auditor.
	10. For the avoidance of doubt the provisions of GC12 *(Assignment and Sub-contracting)* apply to the delivery of any Data Processing Services.
	11. Without prejudice to GC12, before allowing any Sub-processor to process any Personal Data related to this Schedule 6F, the Provider must:
		1. notify the Co-ordinating Commissioner in writing of the intended Sub-processor and processing;
		2. obtain the written consent of the Co-ordinating Commissioner;
		3. carry out appropriate due diligence of the Sub-processor and ensure this is documented;
		4. enter into a binding written agreement with the Sub-processor which as far as practicable includes equivalent terms to those set out in this Schedule 6F and in any event includes the requirements set out at GC21.16.3;
		5. provide the Co-ordinating Commissioner with such information regarding the Sub-processor as the Co-ordinating Commissioner may reasonably require.
	12. The Provider must create and maintain a record of all categories of data processing activities carried out under this Schedule 6F, containing:
		1. the categories of processing carried out under this Schedule 6F;
		2. where applicable, transfers of Personal Data to a third country or an international organisation, including the identification of that third country or international organisation and, where relevant, the documentation of suitable safeguards;
		3. a general description of the Protective Measures taken to ensure the security and integrity of the Personal Data processed under this Schedule 6F; and
		4. a log recording the processing of the Processor Data by or on behalf of the Provider comprising, as a minimum, details of the Processor Data concerned, how the Processor Data was processed, when the Processor Data was processed and the identity of any individual carrying out the processing.
	13. The Provider warrants and undertakes that it will deliver the Data Processing Services in accordance with all Data Protection Legislation and this Contract and in particular that it has in place Protective Measures that are sufficient to ensure that the delivery of the Data Processing Services complies with Data Protection Legislation and ensures that the rights of Data Subjects are protected.
	14. The Provider must comply at all times with obligations equivalent to those imposed on the Co-ordinating Commissioner by virtue of Seventh Data Protection Principle for so long as the DPA 1998 remains in force and after that time with those set out at Article 32 of the GDPR and equivalent provisions implemented into Law.
	15. The Provider must assist the Commissioners in ensuring compliance with the obligations set out at Article 32 to 36 of the GDPR and equivalent provisions implemented into Law, taking into account the nature of processing and the information available to the Provider.
	16. The Provider must take prompt and proper remedial action regarding any Data Loss Event.
	17. The Provider must assist the Co-ordinating Commissioner by taking appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Commissioners’ obligation to respond to requests for exercising rights granted to individuals by Data Protection Legislation.

**Data Processing Services**

**Processing, Personal Data and Data Subjects**

1. The Provider must comply with any further written instructions with respect to processing by the Co-ordinating Commissioner.
2. Any such further instructions shall be incorporated into this Annex.

| **Description**  | **Details** |
| --- | --- |
| Subject matter of the processing | *[This should be a high level, short description of what the processing is about i.e. its subject matter]* |
| Duration of the processing | *[Clearly set out the duration of the processing including dates]* |
| Nature and purposes of the processing | *[Please be as specific as possible, but make sure that you cover all intended purposes. The nature of the processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc. The purpose might include: employment processing, statutory obligation, recruitment assessment etc]* |
| Type of Personal Data  | *[Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc]* |
| Categories of Data Subject | *[Examples include: Staff (including volunteers, agents, and temporary workers), Co-ordinating Commissioners/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc]* |
| Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data | *[Describe how long the data will be retained for, how it be returned or destroyed]* |

## Appendix J – Incident Management and Reporting

**Procedure for handling and reporting information incidents**

Following the adoption of the GDPR on 25th May 2018, NHS Digital issued *Guide to the Notification of Data Security and Protection* Incidents. This guidance supersedes a *Checklist Guidance for Reporting, Managing and Investigating Information Governance Serious Incidents Requiring Investigation* (June 2013).

The purpose for an incident investigation is to determine the facts concerning the incident and:

* To identify whether any deficiencies in the application of the ICBs policies or procedures and/or the organisation’s arrangements for confidentiality and data protection contributed to the incident or;
* Determine whether a human error has occurred, but not to allocate blame;
* Establish what actually happened and what actions need to be taken to prevent reoccurrence.
* Carry out root cause analysis in order to ascertain the cause and to make recommendations

As part of an initial assessment of an incident, the IG Lead will liaise with the service area / team’s IAO/s and the organisation’s SIRO/Caldicott Guardian to ensure incidents are correctly graded and reviewed.

The IG Lead and responsible IAO/s will establish a process so that all facts are looked at and the investigation will be based on establishing what actually happened and what actions need to be taken to prevent reoccurrence, **but not to allocate blame.** However, in some cases the investigation may identify whether any disciplinary processes may need to be invoked

The decision to notify a data subject will be made by the SIRO and the Caldicott Guardian on the grounds of disclosure, including transparency and the ability to protect against harm. This may include theft or blackmail; weighed against the potential harm that may be caused to the subject if notified of the incident.

Where an incident occurs out of business hours, the designated on-call officer will ensure that action is taken to inform the appropriate contacts within 24 hours of becoming aware of the incident.

**Staff Guideline on Identifying and Reporting an Information Incident**

This guideline applies to all staff including permanent, temporary and contract staff. All incidents must be reported to your line manager, Information Asset Owners (IAOs) within 24 hours of becoming aware of the incident.

**What should you report?**

There are three types of breaches:

Confidentiality Breach – unauthorised or accidental disclosure of, or access to personal data.

Availability breach – unauthorised or accidental loss of access to, or destruction of, personal data.

Integrity breach – unauthorised or accidental alteration of personal data.

Here are some examples of information incidents that should be reported:

* Finding a computer printout of Personal Confidential Data (PCD) details laying around;
* Identifying that a fax that was thought to have been sent to a recipient had been received by an unknown recipient or organisation;
* Finding confidential waste in a ‘normal’ waste bin;
* Losing a mobile computing device with personal information on it;
* Giving information to someone who should not have access to it – verbally, in writing or electronically;
* Accessing a computer database using someone else’s authorisation for example someone else’s user id and password;
* Trying to access a secure area using someone else’s swipe card or pin number when not authorised to access that area;
* Finding your PC and/or programmes aren’t working correctly – potentially because you may have a virus;
* Sending a sensitive e-mail to an unintended recipient or ‘all staff’ by mistake;
* Finding a colleague’s password written down on a ‘post-it’ note;
* Discovering a ‘break in’ to the organisation;
* Discovering unauthorised access to Personal Confidential Data (PCD).

**What happens next?**

Your manager or the IG Lead member will investigate the incident and may wish to speak to you directly as things progress.

**Incident Management and Reporting Flowchart**



## Appendix K – Information Governance Training Needs Assessment

**General**

All staff\* likely to be in post for 3 months or longer, are required to complete the online mandatory IG training module- Data Security Awareness Level 1 within the first month of employment (or within two weeks of joining if they work with person identifiable information).

Further training is required for staff who process personal information, and staff within specific roles as set out below.

\*All Staff: Defined as permanent, temporary (including students), contracted, seconded, Board / Governing Body members (including lay members), patient representatives.

Responsibility for seconded staff lays with the employing organisation for IG Training purposes.

New Starters must complete all IG training relevant to their role as soon as possible after employment commencing. The Data Security Awareness level 1 module specifically, must be completed within their first month or within 2 weeks if they handle Person Identifiable Data (PID) (Handling Personal Information training should also be completed as a priority for these individuals, as soon as practically possible).

This Training Needs Analysis (TNA) sets out what IG Training is required for what staff groups, as part of effective delivery of training program.

**Reporting and Monitoring**

The Information Governance Team monitor and report on compliance for IG Training on a quarterly basis between April and December and then monthly January - March each year. Each ICB is provided with information of staff compliance on a quarterly basis.

**Deadlines**

The TNA outlines the frequency the training needs to be completed. Please note the training year for IG training is NOT the same as the financial year, instead this runs from 1st July – 30th June, to coincide with the submission of the DSPT.

**Review and Amendments**

This IG Training Needs Assessment is approved by the Information Governance Steering Group (IGSG) and reviewed on a 2-yearly basis. However, revisions may be made as and when necessary to comply with the law, best practice guidance and instruction from NHS authoritative bodies.

**Training Needs Analysis - By Course**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Course Name** | **Mandatory or Optional** | **Frequency Training Due** | **How to Access** | **Which Roles to Complete** |
| Data Security Awareness Level 1 | Mandatory | Annually (or within one month of commencing employment for new starters OR within 2 weeks of commencing employment for new starters with access to PID). | E-learning (via Electronic Staff Record- ESR) | All staff |
| Handling Person Identifiable Data (PID) | Mandatory  | 2 Yearly | Face to Face (bookable through IG Team).  | All staff that could potentially come into contact with PID |
| Understanding Information Assets | Mandatory | 2 Yearly | Face to Face (bookable through IG Team).  | Information Asset Owners and Administrators |
| IG Board Development Sessions | Mandatory | Annually | Face to Face at Board Development Sessions. | All Board/Governing Body members |
| Privacy Impact Assessment (PIA) Workshops | Optional | N/A | Face to Face (bookable through IG Team).  | Any staff that may need to complete a PIA |
| SIRO Training | Mandatory | 2 Yearly | Scheduled face to face training (external provider) | SIRO’s and their deputies |
| Caldicott Guardian Training | Mandatory | 2 Yearly | Scheduled face to face training (external provider) | Caldicott Guardian’s and their deputies |
| Data Protection Officer Ongoing Development | Mandatory | Ongoing | Various ongoing training and development | Data Protection Officer |

**Training Needs Analysis - By Role (please see course name above for more information)**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Data Security Awareness Level 1** | **Handling Person Identifiable Data** | **Understanding Information Assets** | **IG Board Development Sessions** | **SIRO Training** | **Caldicott Guardian Training** | **Data Protection Officer Ongoing Development** |
| **All Staff** | X |  |  |  |  |  |  |
| **Staff that could potentially come into contact with PID** | X | X |  |  |  |  |  |
| **Information Asset Owners and Administrators** | X |  | X |  |  |  |  |
| **Board / Governing Body members** | X |  |  | X |  |  |  |
| **SIRO’s and their deputies** | X |  |  | X | X |  |  |
| **Caldicott Guardian’s and their deputies** | X | X |  | X |  | X |  |
| **Data Protection Officer** | X | X |  |  |  |  | X |
| **IG Team** | X | X |  |  |  |  |  |
| **Access to Information Team** | X | X |  |  |  |  |  |