****

**Information Governance Strategy**

**incorporating the**

**Information Governance Framework**

**2023 – 2026**

|  |  |
| --- | --- |
| **Version 3.0 – Review/Approval** | **Date** |
| IGSG | 28/07/2023 |
| AMT | 20/09/2023 |
| GAC | 10/10/2023 |
| PHA Board Approval | 19/10/2023 |
|  |  |
| Next Review Date | 31/12/2026  or sooner if required by PHA Reshape and **Refresh** programme |

## Table of Contents

Page No.

1. Introduction 3
2. Scope of Information Governance 3
3. Purpose 3
4. Benefits 4
5. Objectives 4

1. Information Governance Framework 5
   1. Information Governance Policy Statement
   2. Roles, Responsibilities and Reporting Arrangements
   3. Leadership
   4. Supporting Staff
   5. Communication
   6. Training
   7. Implementation and Performance Monitoring
2. Summary and Conclusion 8
3. Equality and Human Rights Considerations 8
4. Review of Policy 8

Appendix 1 Legislation and Guidance 9

Appendix 2 PHA Information Governance Steering Group (IGSG) 13

Appendix 3 PHA Information Governance Framework 15

Appendix 4 PHA Information Governance Policies & Guidance 17

10.0 Version Control 18

**1.0 Introduction**

The Public Health Agency (PHA) is heavily dependent on the information and records it holds and considers all of the data it processes as an asset. It recognises that its records and information must be appropriately managed, handled and protected to serve its business needs and acts openly, while at the same time ensuring that personal and sensitive data is protected. It must demonstrate compliance with all relevant legislation[[1]](#footnote-1) as well as standards set by the Department of Health (DOH).

In recognising its public accountability, the PHA will make every effort to ensure that information is efficiently managed and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management. The framework will ensure that information is accessible while also ensuring the confidentiality of personal data (client and staff), and corporately sensitive information, through adopting robust security measures to protect that information from accidental loss, accidental disclosure or deliberate unauthorised disclosure.

## 2.0 Scope of Information Governance

The effective use of information is central to the planning and delivery of care across the Health and Social Care Environment. The effective use of information will assist in addressing the Quadruple aim outlined in the Bengoa Report, ‘Systems not Structures’ ie. enhancing patience experience, improving population health, reducing costs and improving the work life of staff.

The Information Governance Strategy sets out the framework to ensure that the PHA meets its obligations in respect of information governance; it will also be the vehicle for improving information governance in the PHA. The Strategy covers the 3 year period from 2023 to 2026 and will be supported by annual Action Plans setting out how it will be implemented. The action plans will be monitored by the Information Governance Steering Group[[2]](#footnote-2), chaired by the Senior Information Risk Owner (Director of Operations) or deputy. A report will be submitted to the PHA Governance and Audit Committee on a regular basis.

## 3.0 Purpose

The general purpose of the Information Governance Strategy is to provide clear direction to the PHA in delivering the requirements of information governance including legislative requirements and associated policies. The strategy will assist in establishing and maintaining a robust and effective Information Governance Framework[[3]](#footnote-3) that allows PHA to fully discharge its strategic duties, ensuring that overall corporate compliance is met both in relation to legal and statutory obligations and in meeting all relevant codes of practice.

The Information Governance Strategy cannot be seen in isolation as information is central to all areas of work in the PHA. It outlines the necessary engagement with PHA

Information Asset Owners, providing specialist advice and support, helping to build robust Information Asset Registers.

Information Governance is also a key element of corporate and clinical governance. This strategy is, therefore, closely linked with other strategies, policies, procedures, guidance and staff training to ensure integration with all aspects of the Agency’s business activities.

## 4.0 Benefits

Benefits of a robust and fully implemented Information Governance strategy can be summarised as follows:

* Ensures that decisions are based on readily accessible, high quality information;
* Ensures that information is held and handled securely, and that personal and sensitive information is safeguarded;
* Reduces risks associated with poor and unregulated systems and processes;
* Reduces data losses and the negative impact such losses have on corporate image;
* Ensures that legal and other DOH requirements are met;
* Supports good corporate governance and underpins the assurance framework and corporate risk register;
* Ensures that information and information assets are managed in a coherent manner reducing duplication of effort and increasing availability.

## 5.0 Objectives

The key objectives of this strategy are to ensure the effective management of Information Governance by:

* Complying with all legislation - Data Protection Act (DPA) 2018 and UK General Data Protection Regulation (GDPR), Environmental Information Regulations 2004
* Complying with DOH recommendations and best practice;
* Establishing, implementing and maintaining policies for the effective management of information;
* Recognising the need for an appropriate balance between openness and confidentiality in the management and use of information;
* Providing assurance that all information risks are identified, managed and, where possible, mitigated;
* Minimising the risk of breaches and inappropriate use of personal data;
* Ensuring that the public are effectively informed and know of their right of access (subject access requests)
* Ensuring that all PHA staff are sufficiently trained and enabled to follow and promote best practice in regard to the management of information;
* Completion of the regional Information Management Assurance Checklist.

## 6.0 Information Governance Framework

The Information Governance Framework[[4]](#footnote-4) is an overarching framework which is intended to pull together the various strands of policy and activity covered by ‘Information Governance’. This is important as there are several policies[[5]](#footnote-5) which impinge on Information Governance. It will enable PHA to set out and promote a culture of good practice around the processing of information and use of information systems throughout the organisation. That is, to ensure that information is handled to ethical and quality standards in a secure and confidential manner. The PHA requires all employees and Non-Executive Board Members (Members) to comply with policies, procedures and guidelines which are in place to implement this framework.

## 6.1 Information Governance Policy Statement

Aclear policy framework is critical to ensuring a coherent approach to Information Governance across all PHA functions and locations. This strategy is supported by a suite of information governance policies[[6]](#footnote-6). All Information Governance related policies will be reviewed and updated as necessary on a regular basis.

## 6.2 Roles, Responsibilities and Reporting Arrangements

* **Chief Executive –** The Chief Executive, as Accounting Officer, has responsibility for ensuring that the PHA complies with its statutory obligations and DOH directives. The Chief Executive is required to provide assurance through the Governance Statement that all risks, including those relating to information, are effectively managed and mitigated.
* **PHA board –** The PHA board is responsible for ensuring appropriate systems are in place to ensure effective Information Governance across all of the services for which PHA is responsible. An Information Governance report (included in the PHA Annual Report) will be presented to the PHA Board annually.
* **PHA Governance and Audit Committee (GAC) –** The GAC has responsibility for providing the PHA Board with an independent and objective review of governance processes and an assurance on the adequacy and effectiveness of the system of internal control within the PHA. It will formally review progress on the implementation of this Strategy on an annual basis.
* **PHA Agency Management Team -** AMT will receive updates on Information Governance matters on both a formal and informal basis via the Director of Operations who fulfils the role of Senior Information Risk Owner (SIRO) and Chair of the Information Governance Steering Group. The Personal Data Guardian (PDG) will also report to AMT on matters relating to patient identifiable information where appropriate.
* **Information Governance Steering Group (IGSG)** - Consisting of representatives from all PHA Directorates (Information Asset Owners or their representatives) the primary function of the IGSG will be to lead the development and implementation of the Information Governance Framework across the organisation. The Group will be chaired by the SIRO and will meet at least three times a year, in line with its Terms of Reference.
* **Senior Information Risk Owner (SIRO) -** The SIRO (Director of Operations) is the focus for the management of information risk at board level. The SIRO will advise the Accounting Officer on the Information Risk aspect of the Governance Statement and will own the overall information risk and risk assessment process. The SIRO is a member of the Regional Cyber Security Programme Board.
* **The Personal Data Guardian (PDG)** *-* The PDG (Director of Public Health/Medical Director) has responsibility for ensuring that the PHA processes satisfy the highest practical standards for handling personal data. The PDG is the ‘conscience’ of the organisation in respect of patient information, and will also promote a culture that respects and protects personal data.  The PDG works closely with the SIRO and Information Asset Owners (IAOs) where appropriate, especially where information risk reviews are conducted for assets which comprise or contain patient/service user information.
* **Information Asset Owners (IAO’s)** - Each IAO is responsible for the processing of data within their area/s of responsibility and must maintain and review, on an annual basis, an information asset register for their Directorate. The IAO is also responsible for the management and addressing of risks associated with the information assets within their function and providing an assurance to the SIRO on the management of those assets. Each PHA Assistant Director is the IAO for their function and also sits on the Information Governance Steering Group.
* **Information Asset Assistant** – The Information Asset Assistant has responsibility delegated from the IAO to support them in the management of the information assets within their function.
* **Assistant Director Planning and Business Services (AD P&B)** - The A/D P&B has responsibility delegated from the SIRO for ensuring that effective systems and processes are in place to address the information governance agenda. The Assistant Director is also the Data Protection Officer.
* **Data Protection Officer (DPO)** - The DPO has responsibility for monitoring and ensuring compliance with this policy, UK GDPR and other, relevant data protection legislation, acting as the contact point with the Information Commissioners’ Office, training staff, advising on data protection impact assessments (DPIAs) and conducting internal audits as necessary across the organisation
* **Senior Operations Manager (Delivery) -** The Senior Operations Manager (Delivery) is operationally responsible for the day to day implementation of all aspects of Information Governance.
* **Records Management Working Group (RMWG)** – Chaired by the Senior Operations Manager (Delivery), this Group will address the Records Management function within the PHA, developing and implementing an effective system across all offices. Membership consists of representatives from each Directorate. Members will, in turn, cascade progress across all teams within their Directorate. The RMWG reports to the IGSG.
* **All Staff** - All staff have a responsibility to comply with this strategy and all information governance policies and procedures including the completion of Information Governance Awareness and Cyber Security mandatory training on an annual basis.

## 6.3 Leadership

Effective leadership is essential to create and nurture a corporate culture conducive to effective Information Governance. A culture of corporate and individual ownership and responsibility is essential when looking to effective compliance with all statutes and codes of practice.

## 6.4 Supporting Staff

Clear accountability arrangements will ensure that staff are accountable for the work that they do and the information assets they process and manage. There should be an open and supportive environment in which errors, mistakes or concerns can be raised immediately, with management and corrective measures implemented swiftly and processes changed accordingly.

This culture will further mitigate risks associated with the handling and processing of sensitive information, both corporate and personal in nature.

## 6.5 Communication

It is important to ensure that staff are aware of Information Governance issues, with updates provided as required. Effective and timely communication of Information Governance matters to all PHA staff is essential if the PHA is to meet the aims and objectives associated with this strategy.

As well as ensuring compliance with this strategy and associated policies and procedures, the wider Information Governance agenda within the Public Sector is a fast moving and quickly developing one. It will often be necessary to communicate new directives or initiatives to staff. Communication to staff must be handled with care to ensure that the message is not lost amongst a wealth of material.

## 6.6 Training

It is also essential to ensure that all staff understand and have the knowledge and skills necessary to put the Information Governance Strategy and associated policies and procedures into operational use. The PHA will ensure that appropriate training is developed and available to up-skill existing staff and for new staff entering the service. This will include the use of the e-learning platform. All staff are required to undertake mandatory Information Governance training. The responsibility for ensuring that staff participate in these programmes rests with the relevant IAO and line managers, with support from the Information Governance Steering Group. Members should also avail of relevant information governance awareness and training.

## 6.7 Implementation and Performance Monitoring

An Information Governance Action Plan will be prepared annually. This will also provide a mechanism by which progress can be monitored. The following reporting arrangements will apply:

* Progress reports on the Information Governance Action plan will be agreed through the Information Governance Steering Group;
* Reports on progress against the Information Governance action plan will be provided to the Governance and Audit Committee following each IGSG meeting;
* Reports to the Agency Management Team as required;
* An annual report will be brought to the PHA board as and when required.

Performance will also be monitored annually through the Information Management Assurance Checklist (IMAC). The IMAC includes an assurance, signed by the Chief Executive, to be returned to the DoH. An assurance on the management of information risk is also provided through the Mid-Year Assurance Statement and the Governance Statement.

## 7.0 Summary and Conclusion

Information Governance is a vital and integral part of the PHA’s overall Governance programme. The implementation of the Information Governance Strategy and its subsequent policies, procedures, protocols and guidelines will ensure that the PHA has the appropriate framework in place to meet legislative and organisational requirements and it will drive the development and implementation of improvement plans year on year.

## 8.0 Equality and Human Rights Considerations

8.1 This policy has been screened for equality implications as required by Section 75 and Schedule 9 of the Northern Ireland Act 1998, and it was found that there were no negative impacts on any grouping. This policy will therefore not be subject to an Equality Impact Assessment.

8.2 This policy has been considered under the terms of the Human Rights Act, 1998, and was deemed to be compatible with the European Convention Rights contained in that Act.

8.3 This policy is included in the PHA’s Equality Screening Documentation.

## 9.**0** Review of Policy

9.1 The PHA is committed to ensuring that all policies are kept under review to ensure that they remain compliant with relevant legislation.

9.2 This policy will be reviewed by December 2026, or earlier if relevant guidance is issued.

## Appendix 1

## Legalisation and Guidance

There are a number of pieces of legislation and guidance which have a significant impact on records management and information governance. A selection of these is listed below.

**Public Records Act (Northern Ireland) 1923**

All HSC records ·are public records under the terms of the Public Records Act (Northern Ireland) 1923. Chief Executives and senior managers of all Health and Social Care organisations are personally accountable for records management within their organisation. They have a duty to make arrangements for the safekeeping and correct disposal (under the Disposal of Documents Order (Northern Ireland) 1925) of those records under the overall supervision of the Deputy Keeper of Public Records whose responsibility includes permanent preservation.

**Data Protection Act 2018 and UK General Data Protection Regulations (GDPR) 2018**

The Data Protection Act (DPA) 2018 places a statutory responsibility on the PHA to protect the personal data, which it holds. In relation to records management this means that the PHA must implement measures to:

* Maintain the accuracy of records held;
* Protect the security of personal data;
* Control access to the personal data; and
* Make arrangements for secure disposal once the record is no longer required.

The UK General Data Protection Legislation (GDPR) gives individuals additional rights about how their personal data is used by organisations and applies to all UK and EU organisations that control and or process personal data. It is based on the premise that individuals (‘data subjects’) should have knowledge of what data is held about them, how it is held, how long for and how it is used.

**Confidentiality and Data Protection Act**

All HSC bodies and those carrying out functions on behalf of the HSC have a common law duty of confidence to patients/clients and a duty to maintain professional ethical standards of confidentiality. Everyone working for or with the HSC who records, handles, stores or otherwise comes across personal information has a personal common law duty of confidence to patients/ clients and to his/her employer. The duty of confidence continues even after the death of the patient/client, or after an employee or contractor has left the HSC.

The Data Protection Act (DPA) 2018 includes electronic and manual records. The Act, which applies to the whole of the United Kingdom, sets out requirements for the "processing" of personal data (i.e. meaning obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data).

A "data subject", namely, a living individual who is the subject of personal data, has a right of access to their personal data and, in certain circumstances, can have their data corrected or even deleted.

The UK GDPR sets out 7 key principles which lie at the heart of data protection, and must be followed by all data controllers and processors:

Personal data shall be:

“(1) processed lawfully, fairly and in a transparent manner in relation to individuals (‘**lawfulness, fairness and transparency’**);

(2) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (‘**purpose limitation’**);

(3) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘**data minimisation’**);

(4) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘**accuracy**’);

(5) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals (‘**storage limitation’**);

(6) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘**integrity and confidentiality’**).”

Additionally,

“(7) The controller shall be responsible for, and be able to demonstrate compliance with, principles (1) – (6) above (‘**accountability**’).”

The Information Commissioner, who has responsibility for the enforcement of this legislation, provides guidance on the application of data protection legislation.

Further information on the Data Protection Act 2018 and UK GDPR is available from the Information Commissioner’s Website (<https://ico.org.uk/>).

**Freedom of Information Act 2000**

The Freedom of Information Act 2000 creates a statutory right of access by the public to all records held by public bodies (with some exemptions). The Act makes provision for the Lord Chancellor to issue guidance on how records systems should be maintained in order to facilitate public access to information held. In particular S46 (1) states:

*"The Lord Chancellor shall issue, and may from time to time revise,* a *code* of *practice providing guidance to relevant authorities* as *to the practice which it would, in his opinion, be desirable for them to follow in connection with the keeping, management and destruction* of *their records".*

The Act was brought fully into force on 1 January 2005. The HSC has two main responsibilities under the Act. The HSC has to maintain its 'Publication Scheme' (effectively a guide to the information which is publicly available) and to deal with individual requests for information.

Anyone can make a request for information, although the request must be made in writing (including email). An Environmental Information Regulation (EIR) request, may, however, be verbal. The request must contain details of name and address of the applicant and the information sought.

The HSC is obliged to produce information recorded both before and after the Act was passed. It is vital that records are held within a structured Records Management system in order to meet the HSC obligations under the Act. It should be noted that the responsibility for responding to information access requests lies with the authority that holds the information. The Act is intended to change the way in which public authorities do business, making them more accountable. The foreword to the Code of Practice on Records Management published by the Lord Chancellor under Section 46 of the Act states:

*"Any freedom* of *information legislation is only as* *good* as *the quality of* *the records to which it provides* access".

This highlights the importance of good Records Management in the PHA.

Further information on the Freedom of Information Act is available from: <https://ico.org.uk/>.

**Good Management, Good Records**

These guidelines offer an overview of the key issues, solutions and best practice for HSC teams to follow when preparing a records management strategy. It represents the joint view of DOH and the Public Records Office (PRONI) view of how records should be administered and sets the standard required of the HSC.

The Disposal Schedule has been approved by PRONI. It sets out minimum retention periods for HSC records of all types, except for GP medical records, and indicates which records are most likely to be appropriate for permanent preservation. It also explains the reasoning behind the determination of minimum retention periods, including legal requirements where relevant.

The Schedule does not replace the requirement for PHA to develop and agree their own disposal schedules with PRONI, however, it should form the basis for such schedules.

<https://www.health-ni.gov.uk/articles/gmgr-records-management>

The PHA has in place a systematic and planned approach to the management of **all** records which ensures that, from the moment a record is created until its ultimate disposal, the PHA can control both the quality and quantity of information it generates; can maintain that information in a manner that effectively services its needs and those of its stakeholders; and can dispose of the information appropriately when it is no longer required.

**Information Management Assurance Checklist (IMAC)**

The PHA will complete the Information Management Assurance Checklist (IMAC) and submit to the Department of Health annually.

Legislation, in particular the Data Protection Act 2018, UK GDPR, Freedom of Information Act 2000, the Environmental Information Regulations (EIR) 2004 and Access to Health Records (Northern Ireland) Order 1993 impact significantly on the record keeping arrangements in public authorities.

**ISO 15489: International Standard on Information and Documentation ­Records Management**

The International Standard on managing recorded information, initially based on an earlier Australian standard, was adopted by ISO in 2001. The Standard acts as an enabler towards accreditation and renewal of IS0 9001 and other quality standards. It also provides a specification against which record management practices may themselves be audited.

Appendix 2

**PHA INFORMATION GOVERNANCE STEERING GROUP (IGSG)**

**Terms of Reference (Reviewed June 2022)**

**Purpose**

The purpose of the PHA Information Governance Steering Group, is to lead the development and implementation of the Information Governance Framework across the organisation. It will report to the PHA Agency Management Team (AMT) and Governance and Audit Committee (GAC) providing assurance for the PHA board on the effectiveness of Information Governance systems and practices within the PHA.

**Remit**

* Ensure that information governance systems are in place across the PHA, in line with the PHA Information Governance Framework and relevant Standards and legislation.
* Develop Strategic solutions to Common Information Governance problems.
* Provide a forum to raise awareness and share experience and best practice in Information Governance.
* Provide direction to the work of Records Management Working Group.
* Act as direct point of contact for Information Governance related issues such as Freedom of Information, Information Security and Data Protection etc.
* Agree and monitor the information governance action plan, ensuring actions are taken forward.

**Working Arrangements**

* The Group will meet at least three times a year.
* The Group may from time to time call upon advisors e.g. ICT Security Manager.
* The Group will be chaired by the SIRO, or his nominated deputy.
* The Governance Manager will provide the secretariat for the meeting.
* The agenda and papers will be issued no less than 3 working days in advance of the meeting. Minutes of meeting will be produced and agreed with the chair prior to issue. Draft minutes will be circulated as soon as possible after the meeting, and brought to the next meeting for approval.
* The Group will review its TOR every three years, or sooner if required.

**Reporting Arrangements**

The Group will report to:

* AMT
* PHA Governance and Audit Committee

**Membership List**

**SIRO**

Director of Operations – Chair

**PDG**

Director of Public Health

**Governance & Audit Committee Representative**

Non-Executive Director

**IAOs**

Please note if an IAO cannot attend, their Deputy IAO, or IAA should attend to represent them. Appendix A provides a more detailed list of IAOs, IAO Deputies and their IAAs.

**Operations**

Assistant Director Planning and Operations

Assistant Director Communications and Knowledge Management

**Public Health**

Assistant Director Health Protection

Assistant Director Screening

Assistant Director Service Development

Assistant Director Health & Social Wellbeing Improvement

Assistant Director Research and Development

**Nursing**

Assistant Director AHP &PPI

Assistant Director Nursing (CYP)

Assistant Director Nursing

Assistant Director Nursing

Assistant Director Nursing

Assistant Director Nursing

(NB. Normally, one Assistant Director Nursing will attend on behalf of all the Assistant Directors in Nursing in addition to the Assistant Director AHP & PPI)

**Health and Social Care Quality Improvement**

Clinical Director HSCQI

**Connected Health**

Programme Director

**SBNI**

Professional Officer

**Governance Team**

Senior Operations Manager (Delivery)

Assistant Governance Manager

Further details on the membership of this Group is available at Appendix A.

## Appendix 3 – PHA Information Governance Framework

|  |  |  |
| --- | --- | --- |
| **INFORMATION GOVERNANCE FRAMEWORK** | | |
| **Heading** | **Requirement** | **PHA Structure** |
| Senior Roles | * IG Lead * Senior Information Risk Owner (SIRO) * Personal Data Guardian (PDG) * Data Protection Officer (DPO) | * The Chief Executive as Accountable Officer has overall accountability for IG and is required to provide assurance that all risks to the PHA are effectively managed. * SIRO for the PHA is Director of Operations   & Chair of the Information  Governance  Steering Group.   * PDG for the PHA is Director of Public Health / Medical Director. * IAOs for the PHA are Assistant Directors within each Directorate. * DPO is the Assistant Director of Planning and Business Services (P&B) |
| Policy | * + Over-arching IG Policy   Data Protection Act, UK GDPR and Data Protection and Confidentiality Policy   * + Organisation Security Policy   + Information Lifecycle Management (Records Management) Policy   + Corporate Governance Policy | * Corporate Governance Framework * Information Governance Strategy Incorporating the Information Governance Framework * Information Governance Policy Statement * Data Protection/Confidentiality Policy * ICT Security Policy * Secure Mobile ICT Equipment * Use of the Internet Policy * Use of Electronic Mail Policy * Use of ICT Equipment Policy * Records Management Policy * Freedom of Information Procedures * Access to Information Policy * Data Breach Incident Response Policy |
| Key Governance Bodies | IG Board/Forum/Steering Group | * PHA Governance & Audit Committee * PHA Information Governance Steering Group * PHA Records Management Working Group |
| Resources | Details of key staff roles and dedicated budgets | * Assistant Director of Planning & Business Services * Senior Operations Manager (Delivery) * Governance Administrative Officer   (NB none of the above 3 posts are full time Information Governance) |
| Governance Framework | Details of how responsibility and accountability for IG is cascaded through the organisation. | * All staff contracts include IG clauses * Staff responsibility set out in IG Strategy * Information Asset Register * Notices on Intranet Site (Connect) |
| Training & Guidance | * + Staff Code of Conduct   + Training for all staff   + Organisation Security Policy   + Training for specialist IG roles | * Code of Conduct * IG e-Learning Training mandatory for all staff * PHA ICT Security Policy * SIRO, PDG and IAO’s training completed |
| Incident Management | Documented procedures and staff awareness | * PHA Risk Management Strategy and Policy * Information Sharing Protocol * Guidance for reporting IG related incidents * Data Breach Incident Response Policy (including reporting mechanisms to GAC) * IG Leaflet * Incident and Near Miss Reporting Policy and Procedure |

*Extract from IM CAS:*

*The Information Governance Framework may be described in a single one page standalone document or incorporated within an over-arching IG Policy or an IG Strategy and should provide a summary/overview of how an organisation is addressing the IG agenda*

## Appendix 4 – PHA Information Governance Policies & Guidance

PHA Information Governance Strategy and Framework 2023 – 2026

PHA Records Management Policy

PHA Short Protocol for the handling of requests for information made under the Freedom of Information Act 2000/Data Protection Act 2018

PHA FOI Act Information Handler’s Guidance

# PHA Freedom of Information Internal Review Procedures

# PHA Data Breach Incident Response Policy

# PHA Data Protection/Confidentiality Policy

# PHA Guidance on transferring hard copy personal information

PHA Access to Information Policy

PHA Data Protection Impact Assessment Policy and Guidance

# PHA Information Governance: What you need to know leaflet

PHA Information Security Leaflet

PHA Email Top Tips Guide

PHA Small Cell Sizes Disclosure Protocol

***Regional Guidance:***

*Cyber Security Policies*

*Use of Digital Recorders*

***Other Guidance:***

*DoH Records Management - Good Management Good Records*

*DoH Code of Practice on protecting the confidentiality of service user information*

Version Control:

|  |  |
| --- | --- |
| Version 2 - Approvals |  |
| IGSG | 06/11/18 |
| GAC | 12/12/18 |
| PHA Board | 20/12/18 |
|  |  |
| Version 1 - Approvals |  |
| IGSG | 13/01/15 |
| GAC | 19/02/15 |
| PHA Board | 19/03/15 |

1. *Appendix 1 Legislation and Guidance*  [↑](#footnote-ref-1)
2. *Appendix 2 PHA Information Governance Steering Group (IGSG) Terms of Reference (TOR)* [↑](#footnote-ref-2)
3. *Appendix 3 PHA Information Governance Framework* [↑](#footnote-ref-3)
4. *Appendix 3 PHA Information Governance Framework* [↑](#footnote-ref-4)
5. *Appendix 4 PHA Information Governance Policies* [↑](#footnote-ref-5)
6. *Appendix 4 PHA Information Governance Policies* [↑](#footnote-ref-6)