****

**Information Governance Strategy**

**April 2012 – March 2015**

|  |  |
| --- | --- |
| **Version** | **1.4** |
| **Approved by** | **IGSG & GAC & PHA board** |
| **Date Approved** | **13/2/12 & 16/2/12 &19/04/12** |
| **Review Date** | **By 2013** |

######

Table of Contents

|  |  |  |
| --- | --- | --- |
|  |  |  |
| 1.0 | Introduction |  |
| 2.0 | Scope of Information Governance |  |
| 3.0 | Purpose |  |
| 4.0 | Benefits |  |
| 5.0 | Principles |  |
| 6.0 | Aims |  |
| 7.0 | Roles, Responsibilities and Reporting Arrangements |  |
| 8.0 | Strategic Framework |  |
| 9.0 | Implementation |  |
| 10.0 | Evidencing Progress |  |
| 11.0 | Conclusion |  |
|  | Information Governance Action Plan 2012-2013 |  |
|  |  |  |
| Appendix 1 | Legal and Professional Obligations |  |
| Appendix 2 | The Data Protection Act 1998 |  |
| Appendix 3 | PHA Information Governance Policies |  |

# 1.0 Introduction

The Public Health Agency is heavily dependent on the information and records it holds. It recognizes that its records and information must be appropriately managed, handled and protected to serve its business needs and act openly while at the same time ensuring that personal and sensitive data is protected. It must also demonstrate compliance with all relevant legislation as well as DHSSPS standards.

In recognising its public accountability the PHA will make every effort to 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 or deliberate unauthorised disclosure.

The Information Governance Strategy sets out the framework to ensure that the PHA meets its obligations in respect of information governance, embedding this at the heart of the PHA. It will also be the vehicle for improving information governance in the PHA. The Strategy covers the 3 year period from April 2012 to March 2015 and will be supported by annual Action Plans setting out how it will be implemented.

**2.0 Scope of Information Governance**

Information Governance is an encompassing term for a number of work areas which have had increased attention over recent years. It brings together all of the legal requirements[[1]](#footnote-1), standards and best practice guidance that apply to the handling and use of information and information assets. It is primarily driven by legislation, including:

* Data Protection Act 1998
* Freedom of Information Act 2000
* Environmental Information Regulations 2004
* Access to Health Records (NI) Order 1993
* Human Rights Act 1998
* Public Records Act 1923
* Disposal of Documents Order 1925
* Re-use of Public Sector Information Regulation 2005
* Computer Misuse Act 1990

Ultimately good information governance will facilitate the achievement of PHA corporate goals and priorities as well as enabling it to discharge its legal obligations.

Information Governance covers the ‘life’ of information including how it is obtained, held, recorded, used, shared, released and destroyed or retained.

This strategy relates to all aspects of information governance including:

* Freedom of Information
* Records Management
* Data protection
* IT and Information security/risk

# 3.0 Purpose

The general purpose of the Information Governance Strategy is to set out the PHA approach to information governance, and topromote a culture of good practice around the processing and management of information and the use of information systems throughout the organization.

All staff are required to comply with the Policies, Procedures, Guidelines and associated Action Plans which are in place to implement this strategy.

The Information Governance Strategy cannot be seen in isolation as information is central to all areas of work in the PHA. Information Governance is also a key element of corporate and clinical governance. This strategy is, therefore, closely linked with other strategies to ensure integration with all aspects of the Agency’s business activities.

Effective and robust Information Governance arrangements allow both the organisation and individual officers to ensure that information, and particularly personal or sensitive information, is handled and used legally, securely, efficiently and effectively thereby enhancing the quality of organisational decision making. The strategy enables the organisation to implement procedures and processes that support efficient and compliant collection, use, storage, retrieval, release and ultimately, the decision on whether to destroy or retain the record for a defined period of time.

**4.0 Benefits**

Benefits of a robust and fully implemented Information Governance strategy include:

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

# 5.0 Principles

The four key principles underpinning this Information Governance Strategy are:

* Openness

Non-confidential information relating to the PHA and its role will be readily available to the public through a variety of media, including the PHA Freedom of Information ‘publication scheme’.

* Legal Compliance

The PHA regards all identifiable personal information[[2]](#footnote-2) relating to patient, client, carers and staff as confidential in both content and nature.

* Information Security

The PHA has established and will maintain policies to promote the effective and secure management of its information assets and resources, both electronic and manual.

* Records Management

The PHA is committed to enabling the establishment of a Corporate Records Management programme that will ensure the confidential nature of the record, the integrity of the record and the availability of the record.

# 6.0 Aims

The overarching aim of this Strategy is the development of effective systems, management procedures and practice whereby information governance requirements are met and established as an integral part of the PHA business and culture.

The four key aims of the Information Governance Strategy are:

* To support the work of the PHA by promoting the effective and appropriate use of information.
* To ensure that the PHA complies with relevant legislation in respect of obtaining, handling, processing, storing and disposing of information.
* To develop and provide staff with appropriate tools and support to enable them to carry out their responsibilities in respect of information governance to consistently high standards.
* To enable the PHA to understand its own performance in respect of information governance and manage improvement in a systematic and effective manner.

# 7.0 Objectives

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

* Complying with all relevant legislation.
* Establishing, implementing and maintaining policies for the effective management of information.
* Ensuring a consistent approach within the PHA with regard to information management.
* Ensuring an appropriate balance between openness and confidentiality in the management and use of information.
* Ensuring all PHA staff follow and promote best practice.
* Developing an Information Governance culture throughout the PHA.
* Minimising the risk of inappropriate use or breaches of personal data.
* Ensuring that information risk is managed
* Ensuring maintenance or year on year improvement in line with DHSSPS guidance and models of best practice.

## 8.0 Roles, Responsibilities and Reporting Arrangements

* **All Staff** - All staff have a responsibility to comply with this Strategy and all information governance policies and procedures.
* **Chief Executive –** The Chief Executive, as Accounting Officer, has responsibility for ensuring that the PHA complies with its statutory obligations and DHSSPS directives.
* **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 Statement of Internal Control and will own the overall information risk and risk assessment process.
* **Assistant Director Planning and Operational Services (AD P&OS)**- The AD P&OS has responsibility delegated from the SIRO for ensuring that effective systems and processes are in place to address the information governance agenda.
* **Governance Manager -** The Governance Manager is operationally responsible for the day to day implementation of all aspects of Information Governance.
* **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 where appropriate, especially where information risk reviews are conducted for assets which comprise or contain patient/service user information.
* **Information Asset Owners (IAO’s)** - The IAO’s primary role will be to manage and address risks associated with the information assets within their function and to provide assurance to the SIRO on the management of those assets. Each PHA Assistant Director is the IAO for their function and also sit on the Information Governance Steering Group.
* **Information Asset Assistants (IAA’s)** – IAAs may be identified in each function to support the IAO.
* **Information Governance Steering Group (IGSG)** - Consisting of representatives from all PHA Directorates 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 on a quarterly basis.
* **Records Management Working Group (RMWG)** – Chaired by the Assistant Director of Planning and Operational Services 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.
* **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 PDG will also report on matters relating to patient identifiable information where appropriate.
* **PHA Governance and Audit Committee (GAC) –** The GAC has responsibility for providing the 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 and Action Plan initially on a quarterly basis. A Progress report will be brought to the PHA board for noting at least annually.

**9.0 Strategic Framework**

## 9.1 Policies and Procedures

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[[3]](#footnote-3). All Information Governance related policies will be reviewed and updated as necessary on a regular basis.

##  9.2 Leadership and Culture

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

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.

## 9.3 Communication

It is important to ensure that staff are aware of Information Governance issues, with updates 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, and it will be necessary to communicate new directives or initiatives to staff. Communicating matters to staff must be handled with care to ensure that the message is not lost amongst a wealth of material.

## 9.4 Training

It is also essential to ensure that all staff understand and have the knowledge and skills 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 new staff entering the service. This will include the use of the e-learning platform. In order to ensure that staff are kept up to date and maintain their information knowledge skills, it is important to hold regular ‘refresher’ training; all staff are required to undertake this training regularly.

Where required, the PHA will look at identifying specialist training, for example, in the delivery of an Electronic Document Records Management System solution, for the nominated Data Guardian, Senior Information Risk Owner or Information Asset Owners.

# 10.0 Implementation

The Information Governance Strategy will be supported by an Action Plan setting out how it will be implemented. The Information Governance Action Plan will be reviewed and further developed on an annual basis to ensure that the aims and objectives identified in this strategy are met.

## 11.0 Evidencing Progress

Progress reports on the Information Governance Strategy Action Plan will be the main mechanism for monitoring progress. Quarterly reports will be brought to the Information Governance Steering Group and the Governance and Audit Committee, with reports to the Agency Management Team as required. An annual report will be brought to the PHA board.

Additionally, as identified in the Action Plan, key performance indicators for information governance will be developed and monitored over the course of the life of this Strategy.

Annually, the PHA is assessed against a set of standards and targets in the form of the Controls Assurance Standards (CAS). This currently applies to the Information Governance function directly through the Records Management CAS however, a number of standards are indirectly supporting Information Governance, and its compliance. These CAS are Information Communication Technology (ICT), Waste Management and Security Management. The PHA is required to achieve substantive compliance with all Controls Assurance Standards and report on these annually to the DHSSPS.

Information Governance is also a specific element of the Statement on Internal Control providing assurance in respect of information risk.

# 12.0 Conclusion

Information Governance is a vital and integral part of the PHAs 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.

# 8.0 Information Governance Action Plan 2012-2013

| **Work Area** **/ Topic** | **Action** | **Responsibility** | **Implementation****Date** |
| --- | --- | --- | --- |
| Access to Information | * Compliance with Legislation
* Maintain live database of information requests
* Reporting on FOI requests to IGSG and DHSSPS
* Review and keep up to date Publication Scheme and information made publically accessible via PHA website -
 | Governance Manager / SIRO /PDG/IAOsGovernance ManagerGovernance ManagerGovernance Manager/ Communications Manager | OngoingOngoingongoingongoing |

| **Work Area** **/ Topic** | **Action** | **Responsibility** | **Implementation****Date** |
| --- | --- | --- | --- |
| Information Security / Risk | * Introduce and carry out programme of Office Checks/Inspections.
* Review of IT Equipment – encryption, access, storage.
* Register of Data Access Agreements for all requests to access PHA data by third parties.
* Develop a register of Information Assets
* Identify and Map Information Flows Into and Out Of Information Assets
* Carry out risk assessments of the Information Assets/Information Flows in respect of Information Held, Access, Storage, Transfer, Access Agreements etc.
* Develop guidance on the use of Social Networks and Blogging
* Develop Remote Access Policy
 | Governance ManagerGovernance Manager / BSO ICT Security TeamGovernance ManagerInformation Asset Owners/ Governance Manager Information Asset Owners/ Governance Manager Information Asset Owners/ Governance Manager Governance Manager/ Communications ManagerGovernance Manager/ BSO ICT | OngoingOngoing31/03/201231/03/201231/03/201230/06/201231/03/201230/06/2012 |

| **Work Area** **/ Topic** | **Action** | **Responsibility** | **Implementation****Date** |
| --- | --- | --- | --- |
| Records Management**(See Separate Records Management Strategy & Action Plan)** | * Develop and implement a Records Management Strategy & Action Plan
* Adoption and Implementation of Good Management Good Records
* Provide Appropriate Staff Guidance – Introduction of standardised Records Management Policy, Procedures and Practices across PHA for all stages of the Record Life Cycle.
* Review Record Storage (implementation of above Strategy, Policies and Procedures) – including Retention and Disposal.
* Review Record Security – Physical and Electronic Security of Records.
 | Assistant Director/ Governance Manager / Records Management Working Group | 28/02/2012 and ongoingJanuary 201231/03/2012 and ongoingNov 2011 and ongoingongoing |
| **Work Area** **/ Topic** | **Action** | **Responsibility** | **Implementation****Date** |
| Information Governance | * Develop and implement an Information Governance Strategy and action plan.
* Review and revise all Information Governance Policies and procedures
* Develop appropriate performance indicators for information governance
* Ensure appropriate training is made available to all staff members (Induction, and annual training via e-learning platform), monitor uptake, revise and update training as required
* Specialist training for IGSG Members and Information Governance Staff as required.
* Develop and implement an Information Governance Communications Strategy
 | Information Governance Steering Group.IGSGIGSGGovernance Manager /IGSGGovernance Manager/ IGSGGovernance Manager/ IGSG | 31/03/2012 and ongoing30/06/201230/09/2012OngoingAs required30/06/2012 |

## Appendix 1 - Legal and Professional Obligations

There are a range of legal and professional obligations that limit, prohibit or set conditions in respect of the management, use and disclosure of information and, similarly, a range of statutes that permit or require information to be used or disclosed.

The key legal and professional obligations covering personal and other information listed in this Appendix are as follows:

* [The Access to Health Records (Northern Ireland) Order 1993](http://www.legislation.gov.uk/nisi/1993/1250/contents/made)
* [The Access to Personal Files and Medical Reports (Northern Ireland) Order 1991](http://www.legislation.gov.uk/nisi/1991/1707/contents/made)
* Administrative Law
* [The Adoption Agencies Regulations (Northern Ireland) 1989](http://www.dhsspsni.gov.uk/print/index/hss/child_care/adoption/adoption_guidance_and_regulations.htm)
* [The Blood Safety and Quality Regulations 2005 (as amended)](http://www.uklaws.org/statutory/instruments_34/doc34240.htm)
* [The Census (Confidentiality) (Northern Ireland) Order 1991](http://www.legislation.gov.uk/nisi/1991/760/contents/made)
* [The Civil Evidence (Northern Ireland) Order 1997](http://www.legislation.gov.uk/nisi/1997/2983/introduction?timeline=true)
* The Common Law Duty of Confidentiality
– Confidentiality: [DHSSPS code of practice (PDF 111KB)](http://www.dhsspsni.gov.uk/print/codeofpracticeleafletmay2009.pdf)
* [The Computer Misuse Act 1990](http://www.legislation.gov.uk/ukpga/1990/18/contents)
* [The Congenital Disabilities (Civil Liability) Act 1976](http://www.legislation.gov.uk/ukpga/1976/28/contents/enacted)
* [The Consumer Protection (Northern Ireland) Order 1987](http://www.legislation.gov.uk/nisi/1987/2049/contents/made)
* [The Control of Substances Hazardous to Health Regulations (Northern Ireland) 2003](http://www.legislation.gov.uk/nisr/2003/34/introduction/made?view=plain)
* [The Copyright, Designs and Patents Acts 1988](http://www.legislation.gov.uk/ukpga/1988/48/contents)
* [The Data Protection Act (DPA) 1998](http://www.legislation.gov.uk/ukpga/1998/29/contents)
* [The Data Protection (Processing of Sensitive Personal Data) Order 2000](http://www.legislation.gov.uk/uksi/2000/417/contents/made)
* [Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community Code Relating to Medicinal Products for Human Use](http://www.ema.europa.eu/pdfs/human/pmf/2001-83-EC.pdf)
* [The Electronic Communications Act 2000](http://www.legislation.gov.uk/ukpga/2000/7/notes/contents)
* [The Environmental Information Regulations 2004](http://www.opsi.gov.uk/si/si2004/draft/20040331.htm)
* [The Foster Placement (Children) Regulations (Northern Ireland) 1996](http://www.legislation.gov.uk/nisr/1996/467/introduction/made?view=plain)
* [The Freedom of Information Act (FOIA) 2000](http://www.legislation.gov.uk/ukpga/2000/36/contents)
* [The Gender Recognition Act 2004](http://www.legislation.gov.uk/ukpga/2004/7/section/22)
* [The Gender Recognition (Disclosure of Information) (England, Wales and Northern Ireland) (No. 2) Order 2005](http://www.legislation.gov.uk/uksi/2005/916/contents/made)
* [The Health & Personal Social Services, General Dental Services (Amendment) Regulations (Northern Ireland) 2008](http://www.legislation.gov.uk/nisr/2008/395/contents/made)
* [The Health & Personal Social Services, General Medical Services Contracts Regulations (Northern Ireland) 2004](http://www.legislation.gov.uk/nisr/2004/140/contents/made)
* [The Health and Safety at Work (Northern Ireland) Order 1978](http://www.legislation.gov.uk/nisi/1978/1039)
* [The Health and Social Services (Reform) Act (Northern Ireland) 2009](http://www.legislation.gov.uk/nia/2009/1/notes/contents)
* [The Human Fertilisation and Embryology Act 1990, as amended by the Human Fertilisation and Embryology Act 2008](http://www.legislation.gov.uk/ukpga/2008/22/contents)
* [The Human Rights Act 1998](http://www.legislation.gov.uk/ukpga/1998/42/contents)
* [The Limitation (Northern Ireland) Order 1989](http://www.legislation.gov.uk/nisi/1989/1339/schedule/3/made?view=plain)
* [Police Act 1997](http://www.legislation.gov.uk/ukpga/1997/50/contents) and the [Memorandum to A Code of Practice for Third Party recipients of Criminal Record Information](http://www.dojni.gov.uk/index/accessni/support/code_of_practice_-_amended_for_12_october-5.doc)
* [The Privacy and Electronic Communications (EC Directive) Regulations 2003](http://www.legislation.gov.uk/uksi/2003/2426/contents/made)
* [Public Health Act (Northern Ireland) 1967](http://www.statutelaw.gov.uk/content.aspx?LegType=All+Legislation&searchEnacted=0&extentMatchOnly=0&confersPower=0&blanketAmendment=0&sortAlpha=0&PageNumber=0&NavFrom=0&parentActiveTextDocId=1908736&ActiveTextDocId=1908736&filesize=120977)
* [The Public Interest Disclosure (Northern Ireland) Order 1998](http://www.statutelaw.gov.uk/content.aspx?LegType=All+Legislation&searchEnacted=0&extentMatchOnly=0&confersPower=0&blanketAmendment=0&sortAlpha=0&PageNumber=0&NavFrom=0&parentActiveTextDocId=1922108&ActiveTextDocId=1922108&filesize=57516)
* [The Public Records Act (Northern Ireland) 1923](http://www.statutelaw.gov.uk/legResults.aspx?LegType=All+Legislation&title=freedom+of+information&Year=2000&searchEnacted=0&extentMatchOnly=0&confersPower=0&blanketAmendment=0&TYPE=QS&NavFrom=0&activeTextDocId=1876329&PageNumber=1&SortAlpha=0)
* [Disposal of Documents Order (Northern Ireland)1925](http://www.proni.gov.uk/index/professional_information/legislation.htm)
* [The Radioactive Substances Act 1993](http://www.legislation.gov.uk/ukpga/1993/12/contents)
* [The High-activity Sealed Radioactive Sources and Orphan Sources Regulations 2005](http://www.legislation.gov.uk/uksi/2005/2686/contents/made)
* [The Re-use of Public Sector Information Regulations 2005](http://www.legislation.gov.uk/uksi/2005/1515/introduction/made)
* [The Sexual Offences (Amendment) Act 1992 (as amended by the Youth Justice and Criminal Evidence Act 1999)](http://www.legislation.gov.uk/ukpga/2003/42/schedule/6)

**Relevant Standards and Guidelines**

* BSI DISC BIP 0008
* BS 5454:2000
* BS ISO/IEC 17799:2005 BS ISO/IEC 27001:2005 BS 7799-2:2005
* ISO 15489
* ISO 19005 – 1:2005
* The Records Management Controls Assurance Standard
* The Northern Ireland Records Management Standard

**Professional Codes of Conduct**

* British Association of Social Workers
* British Dietetic Association
* British Orthoptic Society
* The British Dental Association (BDA) Northern Ireland
* The British Medical Association (BMA) Northern Ireland
* The British Association of Occupational Therapy and College of Occupational Therapy
* The Chartered Society of Physiotherapy: Rules of Professional Conduct
* The General Dental Council
* The General Medical Council
* The Health Archives Group (HAG)
* Health Professions Council
* NI Social Care Council: Codes of Practice for Social Care Workers and Employers
* The Nursing and Midwifery Council
* The Pharmaceutical Society of Northern Ireland
* The Royal College of General Practitioners
* The Royal College of Pathologists
* The Royal College of Physicians
* The Royal College of Surgeons of England
* The Royal College of Speech and Language Therapists
* The Society of Chiropodists and Podiatrists
* The Society and College of Radiographers

### Appendix 2 – Personal information as defined by the Data Protection Act 1998

### The Data Protection Act (DPA) 1998

The Act regulates the processing of personal data, held manually and on computer. It applies to personal information generally, not just to health records, therefore the same principles apply to records of employees held by employers, for example in finance, personnel and occupational health departments.

**Personal data** is defined as data relating to a living individual that enables him/her to be identified either from that data alone or from that data in conjunction with other information in the data controller’s possession. It therefore includes such items of information as an individual’s name, address, age, race, religion, gender, and physical, mental or sexual health.

**Processing** includes everything done with that information, i.e. holding, obtaining, recording, using, disclosure and sharing it. Using includes disposal, i.e. closure of the record, transfer to an archive or destruction of the record.

The Act contains three key strands. These deal with:

* notification by a data controller to the Information Commissioner;
* compliance with the eight data protection principles; and
* observing the rights of data subjects.

**Notification by a data controller**

The data controller is the person who determines how and why personal information is processed.  The action of notification can be delegated to the most appropriate person within the organisation, for example the information management, or information governance lead.

Notification is the process of informing the Information Commissioner of the fact that processing of personal data is being carried out within a particular organisation. Its purpose is to achieve openness and transparency – notification entries are placed in a register so that members of the public can check the type of processing being carried out by a particular organisation. The notification process involves completion of a form stating the name of the data controller and detailing the types of processing being carried out.

There are three ways to notify

* On the internet
<https://www.ico.gov.uk/cgi-bin//dprproc?page=7.html>
* requesting a notification form
<http://www.ico.gov.uk/upload/documents/library/data_protection/forms/request_for_notification_form.pdf>

or

* by telephone
You can telephone the notification helpline on 03031231113 between the hours of 9.00am and 5.00pm

**Compliance with the eight data protection principles**

The eight principles advocate fairness and openness in the processing of personal information. The principles are:

1. Personal data shall be processed fairly and lawfully and must be processed in accordance with at least one of the conditions in schedule 2 of the Act. Where the data being processed is sensitive personal information (such as data relating to the physical or mental health of an individual), it must also be processed in accordance with at least one of the conditions in schedule 3 of the Act.
2. Personal data shall be obtained only for one or more specified and lawful purpose.
3. Personal data shall be adequate, relevant and not excessive for its purpose(s).
4. Personal data shall be accurate and where necessary kept up to date.
5. Personal data shall not be kept for longer than is necessary for its purpose(s).
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

## Appendix 3 – Associated PHA Information Governance Policies

# Code of Practice on protecting the confidentiality of service user information

# Data breach incident response policy

# Data protection/Confidentiality policy

# Freedom of Information internal review procedures

# Guidance on transferring hard copy personal information

# Information governance: What you need to know

# Memorandum - Use of unencrypted USB storage devices on PHA computers

# PHA ICT security policy

# Protocol for the handling of requests for information made under the Freedom of Information Act/Data Protection Act

# Records Management - Good Management Good Records

# Records Management Policy

1. Appendix 1 lists the key legal and professional obligations covering personal and other information [↑](#footnote-ref-1)
2. *Appendix 2 Personal information as defined by the Data Protection Act 1998. Note; records relating to an employees work may not fall within the definition of personal information.* [↑](#footnote-ref-2)
3. *Appendix 3 Associated PHA Information Governance Policies* [↑](#footnote-ref-3)