Information Governance and Assurance Framework

Title:	Information Governance and Assurance Framework
Original author(s):	Head of Business Technology
Owner:	SIRO
Reviewed by:	SIRO Group
Approval body:	SIRO Group
Approval date:	
Review frequency:	Annual
Next review date:	January 2019

Change History				
Version	**Date**	**Status**	**Update by**	**Comment**
0.1	04/01/2017	Draft	Head of Business Technology	Initial draft
0.5	12/04/2018	Draft	Data Protection Lead	Changes in IPSA and clarity
1.0	27/04/2018	Published	Data Protection Lead	SIRO comments

1. Introduction

1.1. Purpose and context of the framework

The purpose of the Information Governance and Assurance Framework (the Framework) is to formally establish IPSA's position regarding Information Governance and Assurance.

Information Governance describes the holistic approach to managing information by implementing processes, roles, controls and metrics that treat information as a valuable asset. At IPSA it involves the work of the DPO, Information Technology, and FOI teams. Important consideration should be given to different kinds of information through type and security classification, as well as recognising the value of corporate memory, formally controlled records, and operational guidance.

Information Assurance defines and applies a collection of policies, standards, methodologies, services, and mechanisms to maintain mission integrity with respect to people, process, technology, information, and supporting infrastructure. It is the practice of managing appropriate levels of availability, integrity and confidentiality – whether information is in storage, processing or transit, and if it is threatened by malice or accidental error, fraud, privacy violation, service interruption, theft or disaster.

The intent is to consolidate our Information Governance and Assurance arrangements and risk mitigation measures into one central source. The Framework therefore details the people, places and processes which are in place to ensure that the all staff have access to the relevant information when needed.

The Framework is a baseline for Information Governance training and awareness and sets out the policies and procedures all staff need to understand and apply in the course of their day-to-day work.

1.2. Framework scope

The Information Governance framework covers all staff (including temporary and contract staff) who create, store, share and dispose of information. It sets out the procedures for sharing information with stakeholders, partners and suppliers. It concerns the management of all paper and electronic information and its associated

systems within the organisation, as well as information held outside the organisation that affects its regulatory and legal obligations

1.3. Framework implementation

The SIRO Group will be responsible for the oversight and maintenance of the Framework, with assistance from other specialists in the office, and occasionally external parties.

1.4. Information Governance and Assurance Contacts

There are a number of specialists who have specific responsibility for supporting IPSA's approach to Information Governance and Assurance. In the first instance staff can contact the SIRO, DPO or IT team for support and assistance. See section 4.

2. Information Risk Management

2.1. Risk Management Structure

If we use information well, it helps to make our processes more efficient, improves the services we offer to our stakeholders and improves the quality of our decision making. The risks in handling information are not only in failing to protect it properly, but also in not using it for the public good. Managing information risk is about taking a proportionate approach so that each of these aims are achieved.

Our approach to information risk management is consistent with IPSA's Corporate Risk Policy expressed through the Top Ten risk register where 3 information risks are described: cyber, personal data and IPSA operations information.[check] Since the Cabinet Office review of Data Handling Procedures in Government, there is also a separate but complimentary structure for explicitly managing information risk. In summary:

- Our Audit Committee must now maintain an explicit oversight of information risk, and the Accounting Officer has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level, as well as reporting our status as part of the annual Governance Statement;

- The Senior Information Risk Owner (SIRO) governs the management of information risk at the Executive level. They are also responsible for policy and providing written advice to the Accounting Officer on the content of the annual Governance Statement relating to information risk; and

- The Information Asset Owners are senior individuals involved in running key areas of IPSA. Their role is to understand and address risks to the information; ensure that the information in their business area of IPSA is used legally and for the public good; and provide written assurance to the SIRO on information security and the use of their information assets.

2.2. Our Risk Tolerance

IPSA is not willing to accept information risks that may result in significant reputational damage, financial loss or exposure, information integrity, major breakdowns in information systems or significant incidents or regulatory non-compliance. Generally, IPSA has a cautious approach to risk.

However, IPSA recognises that we cannot eliminate information risk altogether and there may be circumstances where the cost of mitigation outweighs the likely impact of the risk. Our information assurance approach provides the means to identify, prioritise and manage risk and provide a balance between the cost of treating risk and the anticipated benefits that will be derived.

3. Information Assets

3.1. What are Information Assets?

IPSA recognises a number of information asset categories that are central to the efficient running of IPSA – data, software, hardware, services and people.

3.2. Our Information Asset register

Information assets are documented in IPSA's Information Asset Register and each has an Information Asset Owner assigned. Its purpose is to record the organisational areas and process which handle information throughout IPSA. As such it is the foundation for the selection and deployment of our on-going security controls.

It is important to ensure that the register is kept up to date. Changes can be identified via a number of routes, for example and annual risk assessment, a Data Protection Impact Assessment exercise or an Information Governance Audit. The SIRO Group are responsible for ensuring the register is kept up to date.

3.3. Protective Marking Scheme?

IPSA's Protective Marking Scheme is our administrative scheme which helps to ensure that access to information is correctly managed and safeguarded to a commonly understood, and an agreed and proportionate level, including creation, storage, transmission and disposal. The scheme is designed to support our work and meet the requirements of relevant legislation and international standards.

Where a Protective Marking is used, the creator/owner is indicating its sensitivity and the level of security and protection they expect. Staff should be aware of the scheme's markings and associated handling arrangements.

The IPSA Protective Marking Scheme aligns to the UK Government Security Classifications which can be found here - https://www.gov.uk/government/publications/government-security-classifications

IPSA is not currently using a (non-security) classification scheme, but Information Asset Owners must be able to recognise the presence of personal data, and the business processes operating on it. There may be scope to develop a type scheme.

Finally, when working with other parties, IPSA must recognise they may have their own protective marking which may mean a degree of translation is needed. Where possible, IPSA staff should preserve that marking, even when applying our marking.

4. Responsibilities for Information Assurance

4.1. Accounting Officer (AO)

The AO has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level. Information risks should be handled in a similar manner to other major risks such as financial, legal and reputational risk.

Key elements of the Accounting Officer role are:

- Lead and foster a culture that values, protects and uses information for the public good. For example, support the SIRO, participate in training, review and encourage the information assurance approach;

- Discuss information risk in the delivery chain regularly with the internal management team and the IPSA Board; and

- Cover information risk explicitly in the annual Governance Statement.

4.2. Senior Information Risk Owner (SIRO)

The SIRO governs the management of information risk at senior management level. For our purposes, this encompasses our Senior Management Team, which consists of the Chief Executive, Directors and other senior managers.

Key elements of the SIRO role are:

- Lead and foster a culture that values, protects and uses information for the public good. For example, support the IAOs, participate in training, and lead the information assurance approach;

- Define the overall information assurance approach including the Information Governance policies and Information Assurance Framework;

- Own the overall risk assessment process, test its outcome and ensure it is used; and

- Provide assurance to Accounting Officer on IPSA management of information risks and advise the Accounting Officer on the information risk aspects of the annual Governance Statement drawing on assurance statements from IAOs (see below)

4.3. Information Asset Owners (IAO)

IAOs are senior managers involved in running key IPSA business areas. They are responsible for managing risks associated with their information assets. Accountability for information helps to ensure that appropriate protection is maintained. It supports knowing what we are processing, where it is, and why.

IAOs are expected to set the regime for information assurance – as a policy and process owner. Staff are however still responsible for compliance – both with relevant legislation and security policies and procedures.

Key elements of the IAO role are:

- Inform the SIRO of incidents or security risks immediately upon discovery;
- Ensure a segregation of duty is enforced in the application they control; work with IT to enable separation and correct privileges to access systems
- Lead and foster a culture that values and protects information. For example, ensuring staff participate in training and support the information assurance approach;
- Ensure new staff are adequately inducted and briefed on their information security responsibilities;
- Know their information assets e.g. which business processes use it; which systems are used; who has access to it and why; who is the information shared with; and how and when the information is disposed of;
- Maintain an auditable list showing who has and has had access to data in their control;
- Ensure revocation of permissions when a staff member leaves;
- Understand and address risks to their information and provide written assurance to the SIRO annually. For example, contribute to the information risk management procedures and assess the impact of change on an ongoing basis; and
- Ensure the information is fully used for the public good, including responding to requests for access from others. For example, negotiate, manage and approve agreements on the sharing of personal and business sensitive information between organisations; and consider whether better use of the information can be made.

The IAO can delegate day-to-day responsibility for each information asset but overall responsibility remains with the nominated owner of the asset.

In some business areas, IAOs will work with other staff to increase awareness or information assurance procedures and measures. They will be expected to build protection measures in the quality control and operational delivery.

4.4. Managers

All line managers are responsible for ensuring they and their staff are instructed in their information assurance responsibilities, which includes the correct handling or personal and business sensitive information. The responsibility of all managers includes fostering a climate in which staff will give security its due attention.

Practical examples:

- Ensure new staff attend the corporate induction and complete the online Responsible for Information training.

- Ensure all staff know about and understand the Information Governance and Assurance Framework and specifically recognise the importance of Information Governance Policies and supporting procedures and guidance.

- Actively participate in identifying potential information risks in their area and contribute to the implementation of appropriate mitigation.

- Implement the authorisation of access to data (on a need to know / need to use basis) in conjunction with the IAO (according to procedures agreed by the IAO).

Note: Business staff are expected to ensure that only authorised users have access to personal or business sensitive information. If they are in doubt they must seek advice from the manager responsible for the work.

4.5. Staff

All staff must recognise and understand the need to manage proactively the information they create and store. They should consider the value and sensitivity of all the data in their care and take personal responsibility for it.

Practical examples:

- Read the Information Governance and Assurance Framework and understand the Information Governance policies and supporting procedures and guidance.

- Attend Information Governance training, including Data Protection training, annually.

4.6. Information Governance and Assurance staff

IPSA does not have one single Information Governance and Assurance team; instead responsibilities are distributed across the office. Together they support the SIRO.

Collectively, with the SIRO and Data Protection Officer, they are responsible for:

- The co-ordination and operational management of the Information Governance and Assurance approach; leading on continuous improvement for all Information Asset Owner activities; and managing information risks on the IPSA corporate register (3 items: Cyber, data protection, GDPR)

- Reviewing Information Governance and Assurance compliance and ensures quality control and alignment to the Information Assurance Maturity Model and other professional standards; receiving and assessing the Dashboard;

- The creation, monitoring and enforcement of IPSA's Records Management, Retention and Disposal and Information Security policies and associated good practice with awareness through regular training;

- Ensuring IPSA is complying with the six Data Protection Principles, providing advice, guidance and training to staff, procurements and projects involving information requirements; supporting the accountability requirement; promoting the use of Data Protection Impact Assessments for services;

- Handling information security breach incidents; and

The responsibility for the day-to-day management of records is devolved to individual business areas.

The Head of Policy is responsible for:

- Ensuring that IPSA complies with requests for information under the Freedom of Information Act 2000, the Environmental Information Regulations Act 2004, and Subject Access Requests and requests for information under the Data Protection Act 1998/2018 (GDPR);

- Helping to maintain an effective relationship with the Information Commissioners Office and respond to correspondence from that office on complaints about IPSA's handling of information requests; and

- In conjunction with FOI / Data Protection officers, act as a source of advice and expertise to IPSA staff about information legislation generally, including the release of information during an investigation and compliance with the Data Protection Act.

The Head of as IT Security Officer (ITSO) is responsible for:

- Supporting the production of the Information Security Management System (ISMS); accrediting IPSA's ICT systems, accepting residual risk on behalf of the SIRO where it is clearly within IPSA's normal risk appetite;

- Representing security requirements in the procurement, design and implementation of IPSA's ICT architectures, including on premise and cloud software, platform and infrastructure; delivering IT Privacy by Design;

- Conducting technical risk assessments against IPSA's ISMS; and

- Assisting IPSA in the routine application and interpretation of ICT security policies and practices; agreeing the Security Policy and guidance, ICT Acceptable Use Policy and Security Operating Procedures (SyOPs), ensuring these are updated as IT security threats emerge and evolve.

5. Third Party Arrangements

5.1. Contractual Obligations

IPSA uses the information assurance / security elements of the Office of Government Commerce (OGC) model terms and conditions for ICT Services and Contracts, which are the approved Government standards for ICT services contracts and which embody current policy and best practice. IPSA also specifies security requirements in non-ICT services contracts which handle personal and business sensitive information.

5.2. IPSA Suppliers

IPSA has a small number of suppliers who handle personal and business sensitive information on our behalf. IPSA is committed to working with suppliers to drive data handling improvements throughout the delivery chain. Review meetings are held with suppliers periodically to discuss any issues that arise during the course of the contract. These reviews should include assurance metrics and information risk.

Where personal information is exchanged or part of the service, then IT will ensure that relevant security protocols are publicised and that contracts contain relevant provisions under GDPR.

6. Working With Information

6.1. Legal and Regulatory Framework

In managing information risk IPSA will comply with all relevant legislation. The Data Protection Act 2018 (DPA) imposes statutory obligations on anybody processing personal data. The DPA makes clear that IPSA is legally responsible for ensuring that the personal information it creates, uses, stores or otherwise processes must be handled and protected in accordance with the requirements of the DPA.

Parliamentary Standards Act 2009 as amended by the **Constitutional Reform and Governance Act 2010** requires a separation of roles, implementing regulatory and privacy based security measures between Regulation, Administration and Compliance. The IT team must remain observant to this separation and discuss the implications where a potential conflict arises. Nevertheless, when information handling, some operational design may need to accommodate for sharing and case handling to support business functions.

Freedom of Information Act 2000, together with the **Environmental Information Regulations 2004**, establishes a statutory regime for public access to information held by public authorities. The appropriate balance must be struck between this right of access and the need to protect personal and business sensitive information, applying exemptions where legitimate and the public interest is best served by withholding the information.

Other relevant legislation includes the **Computer Misuse Act 1990** and the **Human Rights Act 1998**.

The IPSA Publication Scheme is an approved scheme by the ICO and in 'adopting or reviewing' the scheme may need to seek re-endorsement from the ICO and will need consultation with the Leader of the House of Commons, the Speaker and The House of Commons Committee on Standards and Privileges.

IPSA is working towards achieving appropriate levels in the Information Assurance Maturity Model. Work to modernise and improve information governance and assurance policies and processes will continue and it is expected that we will manage our specific security risks over and above the baseline measures. IPSA is committed to keeping abreast of change and will respond to threat and circumstance appropriately. The Corporate Top 10 Risk Register recognises this.

6.2. Our Information Policies

The purpose of the Information Governance policies is to provide the tools that support the effective use of information and technology while maintaining an environment of controlled risk and value for money investment. In this way the policies aim to enable IPSA to:

- Deliver its strategic priorities;
- Meet its responsibilities to its external stakeholders; and
- Comply with legislation.

The Information Governance policies include (some are embedded within Information Security and the Code of Conduct):

- Clear Desk, Clear Screen Policy
- Website and Cookie Policy
- ICT Code of Conduct, ICT Acceptable Use Policy
- Data Breach Policy
- Information Sharing Policy
- Records Management Policy, Retention and Disposal Schedules
- Information Security Policy, Access Control Policy, Password Policy
- Remote Working and Mobile Device Policy

6.3. Creating and Receiving Information

Information that staff create or receive during the course of their working life is considered as 'recorded information' if held. This includes information originally created by a colleague, another organisation, and a stakeholder or a third party:

- Electronically – for example, an email, Word document, spreadsheet, audio recording, in Microsoft Exchange, shared drives, SharePoint or any other system; or

- Physically – for example, a printed letter, invoice or receipt or handwritten notes.

All recorded information is subject to the Freedom of Information Act 2000 and the Environmental Information Regulations 2004. All recorded personal data is subject to the Data Protection Act 1998/2018. Recorded information must be disclosed on request unless there is a valid exemption for withholding it.

Staff should be aware of information that attracts formal control, and represented within the Information Asset Register, and potential new services that should have a data protection impact assessment before design and entering service.

Staff should always be aware of the type and volume of information they are handling. Further information can be found in the Records Management Policy.

Type and Volume of Information

The type and volume of information created and received will have a direct impact on how staff are expected to handle it – for example, the security arrangements that will be necessary; who will be entitled to access and use the information; and how (if at all) it should be shared outside of IPSA.

In particular, the information staff create and receive may contain the following types of key information:

- Personal information – this relates to individuals, often our stakeholders or staff. See Annex C for ICO guidance on determining what personal data is. Personal information can also be special with additional protection needed.

- Business sensitive information – information that can be considered as business sensitive if IPSA or a third party organisation would be affected by any loss of, or unauthorised access to, the information. For example, information marked as OFFICIAL SENSITIVE under IPSA's Protective Marking Scheme.

The volume of information, along with the nature of the information, can define the risk posed by a breach of security. For example, the loss of one person's bank details, although important, does not have the same impact as losing the bank details of all of our stakeholders; the loss of one person's private address can however cause substantial damage and distress to the individual concerned.

Collecting Personal Information

IPSA would be unable to fulfil many of its functions without collecting personal information from individuals. However, a legitimate need to collect personal information, for example in order to administer an MP's reimbursement claim, provides justification to collect and use personal information, meeting Principle 1 of the Data Protection Act. A Privacy Notice must be provided at the time of collection.

6.4. Storing Information

Protecting Information – a layered approach

Once information is captured it must be protected. Security involves a number of distinct measures which form part of a 'layered' approach. The approach starts with the protection of the information asset at its source, for example protecting the ICT

assets, and then proceeds progressively outwards to include security measures at IPSA's office.

IPSA has a number of policies and procedures which staff must follow to assist with this layered approach. Examples include:

- ICT Acceptable Use Policy;
- Security Operating Procedures for Remote Working;
- Control Procedures for ICT administrators covering removable media, backups, secure disposal, security vetting, account creation and deletion and incident response;
- Clear Desk, Clear Screen Policy; and
- Security Guidance.

Storage

Physical information assets such as supporting evidence for reimbursement claims, HR Personnel records, finance or procurement files which no longer require regular access but need to be retained until their retention period has exceeded, should be deposited to the offsite storage facility.

Electronic information assets will remain in situ until their retention period has exceeded when they will be either deleted or migrated to the IPSA Archive for permanent preservation.

IPSA Archive

IPSA has a physical and electronic archive supplier where information assets selected for permanent preservation or within retention periods are kept.

6.5. Sharing Information

Sharing information with colleagues and stakeholders

Information can be shared where appropriate and in line with relevant legislation and internal policies (i.e. Information Sharing Policy). IPSA staff have a responsibility

to ensure that information is secure when it is being shared – whether internally or externally. All movement of information between people, organisations or ICT systems involves an element of risk. At the same time, people have expectations of us whenever we have access, receive or handle information, especially if the information is personal or business sensitive.

Sharing data by hardcopy documents

Internal sharing of hardcopy documents must follow the Protective Marking Scheme and associated handling arrangements. The Clear Desk, Clear Screen Policy must also be followed.

External sharing of hardcopy documents must also follow the Protective marking Scheme and associated handling arrangements. Where personal data is being shared with stakeholders, Information Sharing Agreements in line with ICO best practice must be created, approved and followed.

Any sharing of hardcopies must recognise that they are uncontrolled in the Quality sense and may become out of date quickly. Anything received should be validated.

Sharing data by email

The Protective Marking Scheme and associated handling arrangements must be followed when sharing information by email. Personal or business sensitive information being shared with stakeholders or other third parties on non-secure networks (e.g. Gmail, Hotmail etc.) must be password protected. Guidance on secure emails and how to password protect documents can be found on the intranet.

Sharing data by removable media

Removable media are not permitted, and generally discouraged, please contact the IT team for advice.

Access to the IPSA Network

Access to the IPSA ICT systems can be gained in three ways:

1. From a desktop PC or terminal within IPSA which provides access to an IPSA domain user account. This is subject to the ICT Code of Conduct and Acceptable Use Policy.

2. Remotely using an IPSA provided or personal computer or laptop and a two-factor authentication token, which provides access to an IPSA domain user account. This is subject to the ICT Code of Conduct, Acceptable Use and Remote Working Policies and SyOPs.

3. Using an IPSA provided BlackBerry which provides access to IPSA email and calendar. This requires the user to have an IPSA domain user account and is subject to the ICT Code of Conduct and Acceptable Use Policy and SyOPs.

Access to IPSA systems by third parties is granted following a decision by the IT Security Officer and is usually subject to completion of BPSS checks and, where necessary, CTC Clearance.

6.6. Disposing Information

Information Disposal

Information is retained by IPSA to support its operational business functions and to fulfil its legal obligations to comply with legislation. At the end of its operational purpose it must be disposed of securely. This means preserved permanently in the IPSA Archive, transferred to the National Archives or destroyed.

IPSA's Disposal Schedule can be found in the Information Asset Register and details the period of retention and the disposal action necessary to manage the information lifecycle. The retention periods and disposal actions that are detailed in this schedule are supported by legislation and best practice, and should be applied to all information retained by IPSA.

Where possible the retention periods and disposal actions will be undertaken and managed by IPSA's Electronic Document and Records Management System (EDRMS). Where this is not possible, the Information Asset Owner is responsible for the application of the retention period and disposal action detailed in this schedule.

Preservation

Information that is to be retained for an extended period will be subject to the Digital Preservation Policy to reduce the risk of loss through obsolescence and degradation and ensure its ongoing accessibility. Hardcopy records will also be preserved in accordance with best practice standards. IPSA is also aware of a need to preserve corporate memory and uncontrolled information that may be retained indefinitely.

Records selected for Permanent Preservation will be stored in the IPSA Archive prior to transfer to the National Archives.

Information Destruction

Personal and business information must be securely disposed. IPSA has arrangements in place for the secure disposal of information with secure confidential waste bins located throughout the office.

7. Training and Culture

Fostering a professional culture and developing a positive attitude toward managing our information assets is critical to the successful delivery of this framework. Information Assurance must be seen as an integral part of, and key enabler to, effective IPSA business.

Training

All new and existing staff are required to undertake Information Governance training on appointment, and Data Protection and Information Assurance training annually.

Information Asset Owners will receive an IAO briefing on their role and responsibilities on appointment and undertake Information Assurance training offered through Civil Service Learning or the National Archives annually.

The Senior Information Risk Owner will attend regular SIRO network briefings and other training offered by the National Archives. The ISPA Board and Audit Committee will also be provided with relevant training and briefing information..

Guidance

IPSA has provided a range of technical and policy guidance to staff via the intranet and other internal publications. This guidance covers the use, creation, protections, access and disposal of IPSA's information.

Disciplinary Procedures

Breaches of information security could result in disciplinary action. The kind of action will depend on the nature of the breach and will be dealt with in accordance with the Data Breach Policy and, if appropriate, Capability and Disciplinary policies.

The ICT Code of Conduct states that "Inappropriate use of IPSA's ICT assets may result in action being taken under the misconduct procedure and in cases of gross misconduct, this may include dismissal." Evidence will be assembled, and discussed with HR.

8. Incident Reporting, Recovery and Contingency

Reporting Information Losses

Staff should report any loss of paper or electronic information to the Head of IT and their Line Manager, in accordance with the Data Breach Policy. Loss of ICT equipment (including Blackberry's and laptops) should be reported to the IT. The loss of the ICT asset will be logged, risk assessed and a replacement arranged.

At the same time staff should ensure that their Information Asset Owner is also notified of the incident. Unprotected information may need statutory reporting to the ICO.

Incident Management and Escalation

The Data Protection Officer, or other nominated investigator, will assess all information losses by completing a data breach report which will help to determine the sensitivity of the information and impact of potential loss.

The actual and/or potential harm to individuals is the overriding consideration in deciding whether a breach of data security should be reported to the individuals concerned and/or the Information Commissioners Office (ICO). Only the SIRO is authorised to permit the reporting of incidents to the ICO.

The Head of IT will assess and support all technology related incident investigations .

Recovery

IPSA makes daily backups of our corporate systems. Backups will be taken at a point in time (nightly) and therefore will not include any information or files created before the next backup is taken. Desktops are not backed up and staff must not store items there, in line with our Records Management Policy. The backup scheme will be reviewed on the introduction or decommissioning of any IT system.

Business Continuity Management

Information Security is a key element of business continuity management. In the event of a significant interruption to service, IPSA's Business Continuity and specific Business Area Continuity plans will be actioned.

These plans must be tested periodically to provide assurance of the completeness and effectiveness of those plans. IT should define testing often and at least schedule for two disaster recovery scenarios and lessons events per year. Plans should be clear about key contacts, handling media and reputation, and effective continuity of operations.

9. Audit, Monitoring and Review

9.1. Monitoring Information Access and Use

ICT Assets

IPSA is required to ensure that it's ICT Acceptable Use Policy and its other rules and procedures are followed. IPSA also has a legitimate interest in protecting its reputation and communication systems, limiting its exposure to legal liability and ensuring that users conduct themselves and perform their work to the level expected of them. IPSA automatically monitors all users' use of ICT assets on a continuous basis and reserves the right to further monitor users' use of its ICT assets, without advance notice, in accordance with the terms of the Policy. Information obtained as a result of monitoring will not normally be used for purposes other than those for which monitoring was carried out, unless it reveals information that IPSA cannot reasonably be expected to ignore (for example a breach of the ICT Code of Conduct or evidence of criminal activities). All use of ICT evidence in investigations should be discussed with the SIRO and HR.

Information Assets

The SIRO Group monitors and considers reporting of access, use and disposal of information held in our ICT systems.

Data Protection Impact Assessments (PIA) and Information Governance Audit

A Privacy Impact Assessment (PIA) is initiated as a result of a proposed change and is a process whereby potential privacy issues and risks in a project or process are identified and examined, from the perspectives of all stakeholders, and a search is undertaken for ways to avoid or minimise privacy concerns. Information Asset Owners should be instrumental in the completion and approval of a PIA.

An Information Governance Audit seeks to understand all aspects of an existing information asset, for example the type and nature of information involved; who has access and why. The Audit is therefore similar to a PIA but is undertaken on projects/process changes that have already been implemented. Information Asset Owners should be instrumental in the completion and approval of an Information Governance Audit.

9.2. Risk Assessments

Quarterly Assessments

IPSA's Audit Committee and Accounting Officer will review information risk quarterly on the basis of a report from the SIRO on Information Governance compliance in IPSA. The Corporate Risk Register will be reviewed.

Information Asset Owners are expected to contribute to the quarterly risk assessment by completing the IAO quarterly assurance statement. In doing so they identify and, where appropriate, formally accept significant risks introduced when personal or business sensitive information is moved or shared.

Annual Assessments

There will be an annual assessment of information risk which will support the SIRO in providing written assurance/advice on the annual Governance Statement to the Accounting Officer. The assessment will cover the effectiveness of the Information Governance and Assurance programme and will be informed by the written IAO

annual assurance statements and compliance checks carried out as part of the Information Governance Compliance Programme.

Internal Audit inspections should also be taken into consideration.

9.3. External Accountability, Transparency and Progress Reporting

IPSA has published its Privacy Notice on our website which sets out for the public their rights for handling personal information and how they can address any concerns they may have.

Each year IPSA will set out in its Annual Report summary material on information risk, covering the overall judgement in the annual Governance Statement, numbers of information security incidents sufficiently significant for the Information Commissioners Office to be informed, the number of people potentially affected and action taken to contain the breach and prevent recurrence.

9.4. Keeping the Framework Under Review

The framework should be subject to annual review. The review will be carried out by the Data Protection Officer in consultation with the Head of Information Technology, and the SIRO Group who can endorse for publication.

Annex A – Identified IAOs

This information is held in a separate Roles and responsibilities document owned by the SIRO Group.

The Joiner and leavers HR processes will identify and reassign roles as needed.

Annex B – Data Protection Principles

Article 5 of the GDPR lists the data protection principles in the following terms:

https://gdpr-info.eu/art-5-gdpr/

1. Personal data shall be:
    1. processed lawfully, fairly and in a transparent manner in relation to the data subject ('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, in accordance with Article 89(1), 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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('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').

The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Annex C – Determining what personal data is

The Information Commissioners Office has produced guidance, in the form of self-assessment questions, to enable you to determine whether the data you are handling should be considered personal.

1. **Identifiability**
   Can a living individual be identified from the data or from the data and other information in the possession of, or likely to come into the possession of, the data controller?

2. **Meaning of 'relates to'**
   Does the data 'relate to' the identifiable living individual, whether in personal, family, business or professional life?

3. **Data 'obviously about' a particular individual**
   Is the data 'obviously about' a particular individual?

4. **Data linked to an individual**
   Is the data 'linked to' an individual so that it provides particular information about that individual?

5. **The purpose of the processing**
   Is the data used, or is it to be used, to inform or influence actions or decisions affecting an identifiable individual?

6. **Biographical significance**
   Does the data have any biographical significance in relation to the individual?

7. **Does the information concentrate on the individual?**
   Does the data focus or concentrate on the individual as its central theme rather than on some other person, or some object, transaction or event?

8. **Processing which has an impact on individuals**
   Does the data impact or have the potential to impact on an individual, whether in a personal, family, business or professional capacity?