Performance Reporting Guidance

Contents

A. Framework Activities

1. Reported Data

This activity is the compilation of performance data across the areas listed below. The data is consistently recorded using document B1 in the Information Governance Framework to present an accurate picture of how well the Organisation is achieving compliance against information legislation.

The spreadsheet reporting form is designed to be a single repository of all the necessary data, however in practice, data may be recorded and stored on separate systems or registers and the data is transferred to the spreadsheet for the purpose of presenting the report to the reporting audience.

The Senior Leadership team, with advice from other key roles such as the Data Protection Officer may decide to broaden or reduce the areas of reporting, or make alterations to the data which is displayed on the overview tab. Any changes should be recorded in the minutes of the Senior Leadership Team with a rationale behind the decision.

Security Incidents

- Reporting is intended to address the question “what can our performance in managing security incidents tell us about the effectiveness of our information governance controls?”
- Data evidencing an effective incident management process assures the ICO that appropriate Organisational Security Measures are in place.
- The report identifies the number of incidents reported/ identified during the period against the definition of what the Organisation considers a breach of its information policies
- The report identifies the policies that have been breached, the severity of the breach and the actions taken to mitigate and prevent future repeat instances.

Data Reported:

Category	Description
Identified/Reported	How many incidents were reported on which date?
Categorised by type	Broken down by the type of breach
Categorised by risk	Broken down by the severity/ risk score of the breach
Categorised by action	Broken down by the mitigating action to resolve the breach
Closure details	Date of closure and any notes
Reported to ICO	How many incidents resulted in a report to the ICO?
Reported to ICO within deadline	How many incidents reported to the ICO were reported within 72 hours?
Resulting in ICO complaint	How many incidents resulted in an ICO Information Notice?
Completed within ICO deadline	What percentage of ICO Information Notices were responded to within the Notice deadline?
ICO Outcome	What was the outcome on any ICO Decision Notice?
Links to RoPA	Whether the breach relates to an information asset or data flow

Freedom of Information/

Environmental Information Regulation Requests

- Reporting is intended to address the question "what can our performance in managing statutory requests for information tell us about the effectiveness of our information governance controls?"
- High rates of completed FOI and EIRs within the statutory timescales with low rates of internal reviews and regulator complaints evidences compliance to the Regulator with the right to know under the respective acts.

Data Reported:

Category	Description
Received in period	How many FOIs and EIRs were received in the period?
Completed in period	How many FOIs and EIRs were completed in the period?
Completed within statutory limit	How many were completed within the statutory deadline?
Internal Reviews (IR)	How many requests for internal reviews were received?
IR Outcome	What was the outcome of the internal review(s)?
ICO complaints	How many ICO complaints were received?
Completed within ICO deadline	What percentage of ICO complaints were responded to within the ICO's deadline?
ICO Outcome	Results of ICO Decision Notice

Access Requests & Rights

- Reporting is intended to address the question “what can our performance in managing statutory requests for information tell us about the effectiveness of our information governance controls?”
- Reporting includes Subject Access, Subject Access CCTV, Police Requests for Information, Internal Reviews, ICO Complaints, and Data Protection Rights requests
- High rates of completed SARs within the statutory timescales with low rates of internal reviews and regulator complaints evidences compliance to the Regulator with the DPA and GDPR right of access to personal data.

Category	Description
Received in period	How many Requests were received in the period?
Completed in period	How many Requests were completed in the period?
Completed within statutory limit	How many were completed within the statutory deadline?
Complaints	How many requests for complaints were received?
Complaint Outcome	What was the outcome of the complaint(s)?
ICO complaints	How many ICO complaints were received?
Completed within ICO deadline	Percentage of ICO complaints were responded to within the ICO’s deadline?
ICO Outcome	Results of ICO Decision Notice

Training & Communications

- Reporting is intended to address the question “what can our performance in designing and delivering training tell us about the effectiveness of our information governance controls?”
- Data evidencing prompt induction, timely completion of mandatory training and high consumption rates of key learning communications provides assurance to the Regulator that effective Organisational Security Measures are in place.

Category	Description
Inductions completed within period	How many induction sessions were completed within the period?
Number of staff who have completed annual refresher training during the period	How many employees completed eLearning during the period?

Number of adhoc training events	This includes any data protection compliance messages delivered at team meetings, by email, or delivered as part of inset day training sessions.

Information Technology

- Reporting is intended to address the question “what can data about information technology processes tell us about the effectiveness of our information governance controls?”
- Data evidencing well managed data growth assures the Regulator that effective Records Management processes are in place
- Data evidencing well managed access to the Organisation’s data (whether for 3rd Parties or by internal employees only having access to the data they should, for the appropriate time and with appropriate approvals) assures the Regulator that data is securely accessible

Category	Description
Total size of network storage used	Growth or negative growth in the storage space on the organisation’s servers for document storage to determine the effectiveness of retention practices
Total size of email storage used	Growth or negative growth in the storage space on the organisation’s email servers for document storage to determine the effectiveness of retention practices
Storage growth – personal folders	Growth or negative growth in the storage space on the organisation’s personal drives for document storage to determine the effectiveness of policy relating to personal use
3rd party Accounts	Number of accounts of 3rd party employees have in order to access to the organisation’s systems or network
Accounts open	Number of IT accounts currently active
Accounts opened	Number of IT accounts created for directly employed new starters during the period
Accounts closed	Number of IT accounts closed during the period
Admin accounts open	Number of IT administrator accounts currently active
Accounts opened	Number of IT administrator accounts created for directly employed new starters during the period
Accounts closed	Number of IT administrator accounts closed during the period
Penetration testing	A record of when tests were undertaken by your IT provider
Patching	Confirming patching is automatically or manually applied
Disaster recovery in place	Confirming Disaster Recovery arrangements are in place and tested

Business Continuity in place	Confirming Business Continuity Plans are in place and tested
Vulnerability Scans	Confirming Vulnerability Scans are conducted regularly

Records of Processing Activity

- Reporting is intended to address the question “what can our performance in developing and maintaining records of processing tell us about the effectiveness of our information governance controls?”
- A complete and well-maintained record of Assets and Flows evidences to the Regulator that the accountability principle under GDPR is met

Category	Description
Assets reviewed	The number of assets reviewed within the period
Flows reviewed	The number of flows reviewed within the period
Overseas data flows	No of overseas flows identified within the period

Records Management

- Reporting is intended to address the question “what can our performance in managing record keeping activities tell us about the effectiveness of our information governance controls?”

Category	Description

Items in stock	The number of files currently closed
Items reviewed for destruction	The number of files assigned for destruction during review
Items destroyed	The number of files approved for destruction and then destroyed within the period

Surveillance

- Reporting is intended to address the question “what can our performance in managing surveillance activities tell us about the effectiveness of our information governance controls?”

Category	Description
Items on Register	The number of surveillance equipment items listed on the register
Number of Impact Assessments completed	How many Impact Assessments have been completed
Requests from Investigators	The number of requests for surveillance personal data received from third parties

Privacy by Design

- Reporting is intended to address the question “what can our performance in managing privacy impact assessments tell us about the effectiveness of our information governance controls?”

Category	Description
Date of completion	The date a DPIA was completed
DPIA Title	The title/purpose of the DPIA
Number of DPIAs approved by DPO	The number of DPIAs successfully approved by the DPO

Audit

- Reporting is intended to address the question "what can the results of internal and external audits tell us about the effectiveness of our information governance controls?"
- The means of collecting and presenting the data is defined in the scoping of each audit whether internal or external in association with the auditor(s).

Category	Description
Audit Date	The date an audit was completed
Audit outcome	If an audit was completed, the auditor's rating of compliance
Direction	Is the rating an improvement against the previous audit?

Information Sharing Protocols

- Reporting is intended to evidence that protocols are in place where required to support information sharing

Category	Description
Audit Date	The date an audit was completed
Audit outcome	If an audit was completed, the auditor's rating of compliance
Direction	Is the rating an improvement against the previous audit?

2. Reported to:

Data Protection Officer (DPO)

- The DPO role is fully documented and the employee in the role is aware of the role's responsibilities and receives appropriate training to ensure the role is executed effectively. The role profile is documented at Document A2.
- The report data must be presented to the DPO before consideration by the Senior Leadership Team in order to allow the DPO to provide commentary on the data and the standing risks derived from the Risk Register.
- This fulfils the DPO role requirement of advising the School's SLT on privacy law issues.
- The DPO commentary is part of the report that goes forward to SLT
- The School may also periodically allow for employees in other specialist roles to similarly add comment on the data where SLT has deemed this to be of value.

Senior Leadership Team (SLT)

- SLT is the executive body within the school which, in the context of Information Governance, reviews performance data as a standing agenda item at each meeting, making recommendations on policy change, risk approach and strategic direction as a result of the data and associated commentary presented.
- SLT's Information Governance role is formally detailed in their terms of reference
- [Include details of any other formal body who will receive the reports, and their role]

3. Informing Reviews:

Policy Review

- All Information Governance policies are reviewed at least annually, however where a need for amendment is identified (for example during an investigation into a security breach) a new version is approved outside of an annual review by SLT. The management of the Policy set is defined in Document C1.
- SLT may devolve approval for minor policy changes to named roles, obviating the need to request approval from full SLT.
- Policy Owners are responsible for documenting any suggestions made for policy amendments. They feed suggestions into the policy review (or action outside of the policy review if a change is urgently required).
- A Policy Change Log (Document D1) is maintained providing a full explanation of the version changes resulting from amendment approvals. The log records the details of the change, who approved the change and when, and when was the new version published/ communicated to employees.

Risk Review

- The Organisation’s Risk Register (Document G1) is formally reviewed at least annually but the regular reporting to SLT contains the opportunity for the DPO to comment on how the performance data is affecting risk management and for SLT to discuss issues arising at meetings.
- The purpose of the risk review is to determine:
    - whether the risk register captures all risks to Information Governance compliance
    - the assessment of individual risks accurately reflects the potential impact and severity
    - the Organisation has set a risk tolerance against all risks which informs the decisions about mitigating actions

Strategy Review

- The Information Governance Strategy (Document C1) sets out the Organisation’s aspirations for Information Governance over a timeframe typically broader than the annual cycles which apply to policy and risk reviews

- It is important however to revisit progress against the strategy on an annual basis. On a basic level this review can take the form of an informal measure of whether the strategy remains on track. On a more formal level, there could be an annual progress report which notes progress against each requirement, sets out a gap analysis and presents options for improvement.
- A strategy which intends to deliver achievements over a number of years does not need to remain static in its content for that period. Legal changes, technology changes and corporate changes in emphasis may result in a rethink applicable to individual areas of the strategy or major changes to the entire document.
- Where changes to an in-flight strategy are suggested, the approval process is for agreement to be obtained from the same bodies and key individuals who approved the original version having been presented with comprehensive reasons for amendments and consideration of the risks of change and of not making changes.