Information Governance Annual Report 2022 – 2023

Version 1.0

October 2023

Document Control Sheet

Title	Information Governance Annual Report 2022 - 2023						
Author(s)	Information Governance Manager & Data Protection Officer, and, Information Governance Officer						
Consultees	Information Assurance Group, including: Head of Governance, Strategy and Performance Senior Solicitor Solicitor ICT Team Leader and Information Security Officer Audit and Risk Manager						
Version	1.0						
Date	Oct '23						

Contents

1 Purpose

To report on the delivery and continuous improvement of Moray Council's compliance with regulatory regimes relating to Information Governance, with particular focus on Data Protection, Access to Information and Records Management.

This is the first Information Governance report, it is anticipated that hereafter, an Information Governance report will be produced annually.

2 Background

Information Governance covers a range of procedures, policies, and guidance used to support the Council in maintaining compliance with information legislation and its promotion of good recordkeeping; ensuring that the Council's information assets remain secure, relevant and accessible. This applies to the management of all information, in all formats, which the Council may collect, create, handle, store, share, erase, process, archive, and manage in any way. A summary of the relevant legislative regimes and key features is provided in Appendix 1.

2.1 The Information Governance Team

The Information Governance team are responsible for the development, implementation and monitoring of corporate information governance and record management strategies, policies and statutory obligations across the Council, Licensing Board and Moray Integration Joint Board (MIJB).

The Information Governance Team sit within Governance, Strategy and Performance and comprise:

- Information Governance Manager and Data Protection Officer (IGM & DPO for both the Council, and, MIJB)
- Information Governance Officer (IGO)
- Information Co-ordinator (0.7 FTE)

Although Local Heritage and Archives remain under Education Resources and Communities, the IGM, as a qualified Archivist, endeavours to support the development, maintenance and management of Heritage and Archives.

The IGM and IGO are members of:

- the Council's Information Assurance Group (IAG), which has strategic oversight of Data Protection and Information Security issues across the Council.
- SOLAR – DP/FOI/HRA Group.
- ASLAWG (IGM only).

3 Data Protection

In the UK, the protection of personal data is governed by the Data Protection Act 2018 (DPA) and the United Kingdom General Data Protection Regulation (UK

GDPR).[1] UK GDPR is the retained version of the European Union General Data Protection Regulation (GDPR), which came into force 25th May 2018.

In 2018, a range of new measures were implemented by the Council to support compliance with the legislative regime set out under the DPA 2018 and GDPR. The first assessment of these measures by the Council's Internal Audit Service took place in September 2022. The audit sought to provide assurance that the Council had systems and controls in place as required under Data Protection legislation (UK GDPR and the DPA), and that the Council has the appropriate governance arrangements, policies, procedures and training programmes in place, to monitor ongoing compliance. The audit found both the system assessment and testing assessment to be limited.

3.1 Data Breaches

A personal data breach, is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".[2]

The Council's current data breach procedure requires all staff to report data breaches to the Council's data breach team as soon as a breach is identified or reasonably suspected. The data breach team will investigate the breach, assist with containment of the breach and undertake a risk assessment to establish whether the breach meets the threshold for reporting to the Information Commissioner's Office (ICO).

A breach likely to result in a risk to the rights and freedoms of data subject must be reported to the ICO within 72 hours of the Council becoming aware of the breach.[3] The Council 'becomes aware' of a breach the moment any member of staff becomes aware of the breach. Where a breach is likely to result in "a high risk to the rights and freedoms" of the data subject(s), the Council must also report the incident to the data subject(s) concerned.[4]

The Council's Data Breach Reporting Form and Guidance on Data Security Breach Management are available on the Data Protection interchange page: http://interchange.moray.gov.uk/int_standard/Page_132347.html

3.1.1 Data Breach Register

In compliance with UK GDPR Article 33(5), all data breaches are recorded on the Council's Data Breach Register. A record must be maintained of the facts regarding each breach, its effects and remedial action taken.

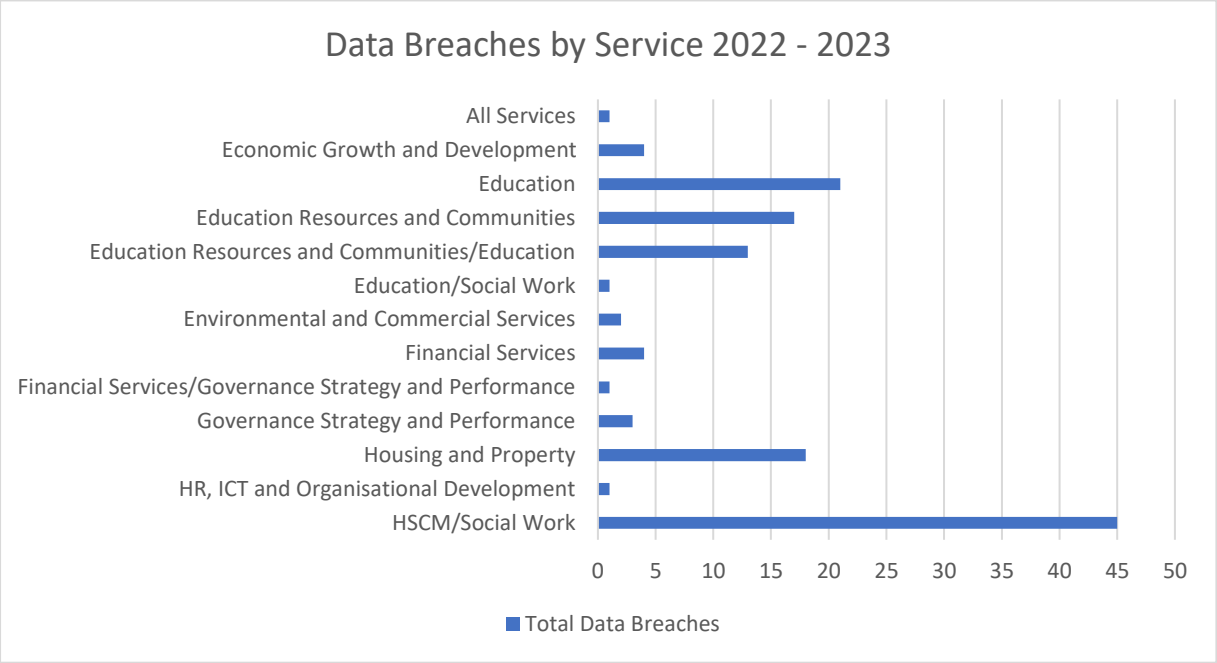
---

[1] Further reform of the UK Data Protection legislative regime is expected via the Data Protection and Digital Information Bill (No.2), introduced to Parliament on 8 March 2023. The full text of the draft Bill and Explanatory Notes is available here: https://bills.parliament.uk/bills/3430
[2] UK GDPR Article 4(12).
[3] UK GDPR Article 33.
[4] UK GDPR Article 34.

All confirmed and suspected data breaches are recorded, investigated and mitigations put in place to reduce the risk of a similar or more significant incident occurring in future.

From Autumn 2021 the Information Governance team started alerting Heads of Services to data breaches that take place within their Services.

131 data breaches were reported and recorded within the Council between April 2022 and March 2023:



3.1.2 The Information Commissioner's Office (ICO)

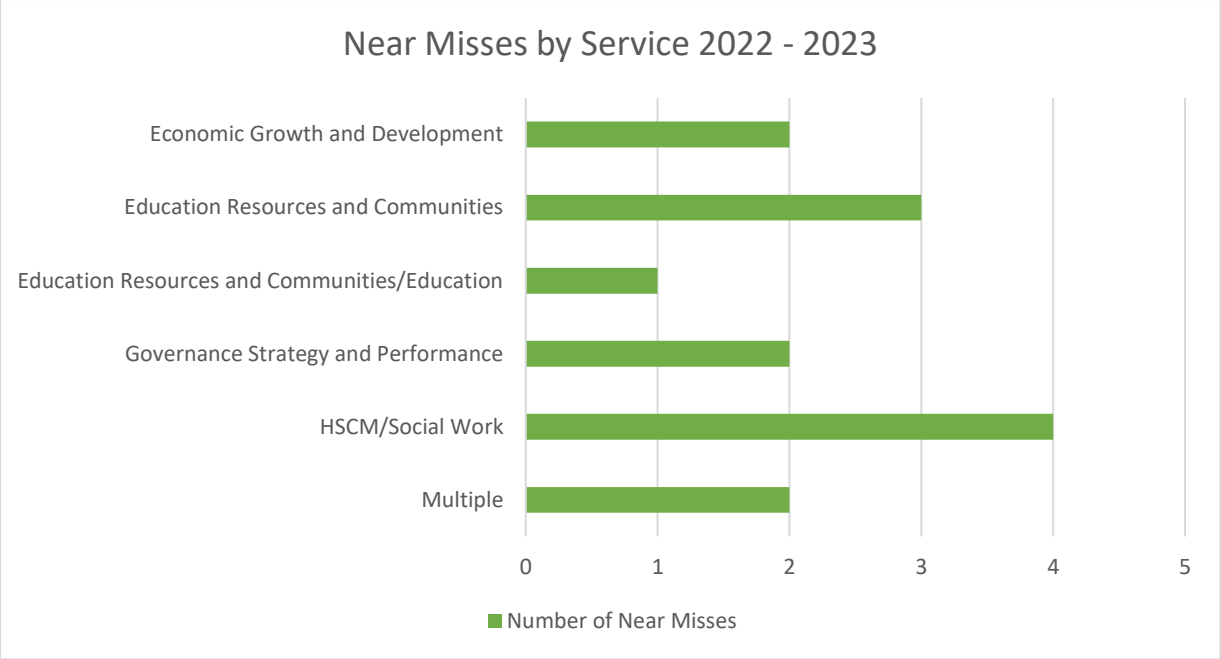
The ICO is the independent supervisory authority for data protection in the UK. They oversee and enforce UK Data Protection legislation. The ICO have significant tools at their disposal to take action for a breach of UK GDPR or the DPA 2018. These include warnings, reprimands, enforcement notices and penalty notices. They have the power to issue fines of up to £17.5 million, or 4% of an organisation's annual worldwide turnover, whichever is greater.

Two data breaches were considered to meet the threshold for reporting to the ICO due to the likelihood of risk to the rights and freedoms of the data subjects. Both breaches were also assessed as meeting the statutory threshold for reporting to the affected data subjects. In both cases, following a review of the information provided about each data breach, the ICO decided that no further action by the ICO was necessary.

3.1.3 Near Miss Data Breaches

Although not a requirement under Data Protection legislation, the data breach team also record 'near-miss' data breaches, so that preventative measures can be put in place to ensure that similar more serious situations do not arise in future.

14 near misses were reported and recorded for 2022/23:



3.1.4 Lessons Learned

Each data security incident is assessed on a case by case basis and suitable, relevant mitigations are discussed with Services to improve information management practices. This should reduce the likelihood of a similar, or more significant, incident occurring in future.

In all instances reported 2022/23, manual, rather than technical measures were put in place. For example, requiring employees to manually check email addresses, attachments, process documents, addresses etc. Such follow up measures place a reliance on the training and knowledge of employees.

Feedback and recommended actions from the ICO in relation to the two reported incidents, combined with findings from the Council's Internal Audit of 'GDPR', are recorded below, in addition to actions taken and planned actions for 2023/24:

The ICO
• Preventative measures in place that should help to reduce the risk of breaches of the nature reported in that instance occurring; including mandatory data protection training, refresher data protection training and targeted training following any 'near-miss' breaches. • Recommended regularly reminding staff about their data protection obligations. • Recommended having clear written guidance in place for all staff, highlighting the confidentiality and data security responsibilities within the organisation.

- Recommend reviewing staff contracts to ensure they clearly outline what staff can and cannot do with the personal data they handle, particularly in relation to handling service user details.
- Recommended reviewing the Council's 'bring your own device' (BYOD) policy, or consider implementing one as soon as feasibly possible to ensure staff who use personal devices have clear guidelines to follow on their use.
- Recommended impact of data breach on data subject is monitored and support offered to mitigate any risk of further detriment, and, that any identified outstanding remedial measures as part of the breach investigation are implemented.

Internal Audit

- Data Protection Policy and guidance should be reviewed and thereafter a timetable for continued review set.
- A Record of Processing Activities (ROPA) should be compiled by the Council based on a data mapping exercise.
- An Information Asset Register (IAR) should be compiled and maintained on an ongoing basis.
- A review of Privacy Notices held within Council services should be progressed and the documents made available on the Council website for public inspection.
- Consideration should be given to undertaking reviews within Services to audit compliance with the Data Protection Policy and Guidance.
- A review of the guidance documents and forms held within the Information Management section of the Interchange should be undertaken and updated accordingly.
- A review should be undertaken of the officers that have not undertaken the data protection training on the LearnPro training system. Those identified should be reminded to undertake their data protection training requirement.
- Consideration should be given to providing elected members with an update of actions undertaken to ensure the Council's compliance with data protection requirements.

Actions being taken:

- Staff are regularly reminded about their data protection obligations via internal reminders on interchange news. Reminders were issued about DPIAs, GDPR and the Data Protection Act 2018, clearing email caches (to mitigate against data breaches involving autofill), data breach reporting, DPIAs, Data Sharing/Processing Agreements.
- A suite of data protection guidance is also available on the interchange Information Governance pages.
- Work is ongoing with Services to compile and complete a thorough ROPA and IAR.
- Work is ongoing with Services to review and update current Privacy Notices. As Privacy Notices are updated or created they are added to a

designated Privacy Notices webpage on the Council website: http://www.moray.gov.uk/moray_standard/page_142831.html • Information Governance report produced to provide elected members with updates on the delivery and continuous improvement of the Council's compliance with data protection legislation 2022/23. • The interchange now has an internally published register of DPIAs, highlighting processes and applications approved (or not) for use. The register is updated monthly and available here: http://interchange.moray.gov.uk/int_standard/Page_132347.html
Planned Actions:
• Schedule of work to be drawn up to prioritise the ongoing reviewing and updating of Information Governance guidance and polices. • Upon completion, both the ROPA and IAR are to be reviewed biennially. • Continue ongoing work with Services to review and update current Privacy Notices, with all updated and new Privacy Notices to be added to the Council's designated Privacy Notice webpage. • An Information Governance report is to be produced annually. • A register of Data Sharing Agreements (DSAs), Data Processing Agreements (DPAs), Information Sharing Protocols (ISPs), Memorandums of Understanding (MoUs) and similar agreements reviewed by the Council's Information Governance Team is to be made available on the interchange. The register will be updated monthly.

3.2 Data Sharing/Processing Agreements

It is good practice for Data Controllers to have written Data Sharing Agreements (DSAs) when controllers share personal data. This helps all parties to understand the purpose for the sharing, what will happen at each stage of the process and what responsibilities they have. Similarly, Data Processing Agreements (DPAs) with any third-party processors can help all parties understand their data protection obligations and provide some legal certainty in areas with significant potential liability. These Agreements also helps the Council to demonstrate compliance in a clear and formal way.

During 2022/23 the IG Team have advised on over 20 DSAs, DPAs, Letters of Variation, Service Level Agreements and Memorandum of Understanding. These are recorded on a central register and copies of all agreements are held in a central repository.

3.3 Data Protection Impact Assessments (DPIAs)

DPIAs are an important tool to help identify and minimise the data protection risks of a project or process. They are required for any processing that is likely to result in a high risk to individuals, as such a screening section at the start of the DPIA form should highlight any such potential high risks. DPIAs also highlight if a new Privacy Notice or DSA/DPA may be required, as such DPIAs must be kept up to date with any significant changes.

65 DPIAs were reviewed in 2022/23, with all but 1 approved. An internally published register summarises any caveats required prior to use and notes why a DPIA may not be approved; it is available on the interchange here: Home > Policies, Procedures & Guidance > Information Governance > Data Protection

3.4 Privacy Notices

Privacy Notices (PNs) are required to inform data subjects how their personal data would be managed should they provide it for a certain process. PNs must clearly cover what personal data is collected, by whom and under which legal basis (bases), how it is handled, stored and shared, when it will be destroyed, and, what data rights may be applied. The IG Team are gradually reviewing and updating all PNs, these are being added to a single, publically accessible webpage: www.moray.gov.uk/privacynotices

3.5 Advice, Guidance and Training

The IG Team provide advice, produce Guidance documents and Training as and when required. 2022/23 has seen a focus on supporting services with handling Data Protection Information Release requests, specifically those from the Police. Targeted training was also delivered, including to Councillors (Summer 2022) and Moray Integration Joint Board (Summer 2022).

4 Access to Information – Requests under FOISA and EIRs

The Freedom of Information (Scotland) Act 2002 (FOISA) and the Environmental Information (Scotland) Regulations 2004 (EIRs) came into force in 2005. Under FOISA, anyone who requests information from a Scottish public authority, which holds it is entitled to be given it by the authority (subject to a limited number of exemptions). FOISA applies to all information held by the Council, regardless of whether the Council created it or received the information from a third party. It covers information regardless of how it is recorded, or its format, for example emails, handwritten notes, photos, CCTV tapes, recorded messages etc. are all covered.

Whilst the EIRs, give the public the right to ask for environmental information held by a Scottish public authority (subject to a limited number of exceptions). Environmental Information covers a broad range of topics, such as the environment itself, and, matters that affect the environment such as emissions, radiation, noise and other forms of pollution and policies.

FOI and EIRs requests for information held by the Council or MIJB are logged, co-ordinated and responded to by the FOI Team (Information Co-ordinator).

FOISA and EIRs are enforced and promoted by the Scottish Information Commissioner (SIC), an independent public official. The SIC is responsible for dealing with complaints, promoting good practice to authorities, informing the public about information legislation and enforcing the relevant legislation. Requestors have the right to appeal to the SIC to make a decision on the response issued by an authority, following the authority's review. The SIC can order an authority to disclose

information, should it find that information has been wrongly withheld. SIC's Decision Notices are legally binding, although an appeal on a point of law may be made to the Court of Session. Appeals are dealt with on a case by case basis; completed cases are reported on the decisions section of the SIC's website.

Should the SIC become aware that an authority is not complying with its duties under freedom of information legislation, the SIC may issue an enforcement notice, to compel compliance within a specific timescale. Failure to do so may result in a referral of the matter to the Court of Session.

5 Access to Information - Subject Access Requests

Under Data Protection legislation, data subjects have a right of access to the personal data about themselves held by an organisation. This is referred to as a subject access request (SAR). A SAR gives data subjects the right to obtain a copy of their personal data, as well as other supplementary information.

The ICO oversees and enforces the right of access. Data subjects have the right to lodge a complaint with the ICO about an infringement of Data Protection legislation in relation to their personal data, such as an organisation's failure to comply with a SAR. If the ICO establishes that an organisation has failed to comply with Data Protection legislation, the ICO may exercise their enforcement powers and issue the relevant organisation with a warning, reprimand, enforcement notice or penalty notice.

Should an organisation fail to comply with a SAR, the requestor may also apply for a court order requiring the organisation to comply, or to seek compensation. It is a matter for the court to decide, on a case by case basis, what action to take.

The co-ordination of this statutory duty is managed by the Information Co-ordinator, who collates the relevant information, organises redaction meetings and arranges of the released information to be collected.

The number of requests received under FOISA, the EIRs and Data Protection legislation have been gradually increasing in number, as illustrated in the table below:

Access to Information Requests 2016 – 2023

Year	FOI requests received	EIR requests received	SAR requests received	Reviews	Notes
2016 – 17	1144	19	31	13	
2017 – 18	1231	28	36	22	
2018 – 19	1321	104	59	21	
2019 – 20	1091	161	52	10	

2020 – 21	880	66	63	12	*Covid legislation extended timescales for release of information.
2021 – 22	1006	59	53	14	*Covid legislation extended timescales for release of information.
2022 – 23	1322	42	91	20	

Since January 2023, access to information statistics are collected in a more rigorous way to better reflect the burden of complying with such requests, see Appendix 2.

6 Records Management

The Public Records (Scotland) Act 2011 (PRSA) requires public authorities to develop and maintain a Records Management Plan (RMP) subject to approval by the Keeper of the Records of Scotland (the Keeper). Section 5(1) of PRSA requires RMPs to be kept under review; with voluntary progress update reviews (PURs), and RMPs to be fully re-submitted every 5 years.

Moray Council's first RMP, which covers the Council and Moray Licensing Board, was accepted by the Keeper on 6 March 2014 on an improvement model basis, with a number of areas highlighted by the Keeper as requiring ongoing improvement and development to close a gap in provision.

The Council's second RMP was submitted December 2020. On 15th July 2022, the Council received the National Records of Scotland's (NRS) PRSA Assessment Team's Interim Report on the Council's 2020 RMP submission. The purpose of the Interim Report is to highlight areas of required improvement before the Keeper agrees to a final plan; it facilitates a discussion with the PRSA Team about the issues highlighted by the assessment.

There are 15 elements to a RMP, with a Red Amber Green acceptance scale. In the Interim Report, the Assessment Team highlighted 3 elements as Green (accepted by the Keeper), 7 elements as Amber (accepted on an 'improvement model' basis) and 5 elements as Red (unacceptable). As such, their recommendation would be that the Keeper formally returns the RMP to the Council as failing to meet the requirements under the PRSA. A response to the Interim Report was submitted September 2023.

Should the Keeper return the RMP to the Council, as failing to meet the requirements under the PRSA, the Keeper may consider invoking their powers under section 7 of the PRSA. Including taking such steps as the Keeper considers appropriate to publicise the failure. This would include alerting Scottish Ministers and inviting the Cabinet Secretary and Minister with responsibility for local authority business to respond and could include publication to appropriate professional publications.

The RMP for MIJB is aligned with the Council's RMP. Ten elements (excluding 1, 9, 13, 14 & 15) on MIJB's RMP are directly covered by the Council's RMP. As such the above noted issues will also affect the IJB's RMP

7 Closed Records Store

The Council's Closed Records Store (CRS) is designed for the secure storage of physical information that is semi-current and requiring retaining. Paperwork, files, photographs, microfilms and other hardcopy information that is no longer in current use, may still be required either for an ongoing business use or to be kept under the Council's Retention Schedules, these are considered a Record and transferred to the CRS.

The CRS was relocated in 2019, then partially relocated in July 2022 and March 2023. There are now three CRS stores in 3 different locations within Moray. These stores and records are managed by the IGM. There is no open access; requested records are retrieved and returned by Mailroom staff.

Since March 2023, nearly half of the CRS's collections are now housed within one location, in a more suitable and accessible building. New mobile racking has been purchased, ensuring that the most recent CRS store is fully utilised. In spite of these improvements, it should be noted that the CRS does not conform to the relevant standards required.

During 2022/23: 684 boxes were accessioned to the CRS.

Space for new accessions remains limited. When records are highlighted by the IGM as due for destruction, relevant Services are contacted to arrange for review of the records, however, due to the IGM's capacity there is currently a backlog of records awaiting review by Services.

Appendix 1 – Information Governance Legislation

Legislation	Key Features
United Kingdom General Data Protection Regulation (UK GDPR)/ Data Protection Act (DPA) 2018	• Governs the protection of personal data in the UK; • Mandatory recording and reporting of personal data breaches. Any breach likely to "result in a risk to the rights and freedoms" of the data subject(s) must be reported to the ICO within 72 hours of the Council becoming aware of the breach (UK GDPR Article 33); • Any breach likely to result in "a high risk to the rights and freedoms" of the data subject(s) must be reported to the data subject(s) (UK GDPR Article 34); • A 'personal data breach' is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed." (UK GDPR Article 4). • Gives data subjects specific rights over the processing of their personal data, including: the right to be informed about the collection and use of their personal data; the right to access personal data held about them; rights to have their data rectified, erased or restricted; the right to object; the right to portability of their data and the right not to be subject to a decision based solely on automated processing. Where the legal basis for processing is consent, data subjects also have the right at any time to withdraw their consent to that processing. • Introduced a duty on public authorities to appoint a Data Protection Officer (DPO). DPOs assist with monitoring internal compliance with Data Protection legislation, informing and advising on Data Protection obligations, approving Data Protection Impact Assessments (DPIAs) and to act as the contact point for the ICO. DPOs must be independent, experts in Data Protection, adequately resourced, and, report to the highest management level. • Sets out seven key principles for processing personal data: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality and accountability. • Under the accountability principle, the Council must have appropriate measures and records in place to demonstrate its compliance with the UK GDPR. This includes: taking a data protection by design approach; maintaining documentation of our processing activities; adopting and

	implementing Data Protection policies and guides; having written contracts in place with organisations who process personal data on the Councils behalf; implementing appropriate security measures; recording and reporting personal data breaches and carrying out DPIAs. These measures and records should be kept under regular review and updated when necessary. • Failure to comply with the principles can result in substantial fines – up to £17.5 million, or 4% of an organisation's total worldwide annual turnover, whichever is higher.
Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR)	• Sits alongside DPA 2018 and UK GDPR; • Sets out specific privacy rights on electronic communications, including: marketing calls, emails, texts and faxes; cookies (and similar technologies); keeping communications services secure; and customer privacy regarding traffic and location data, itemised billing, line identification, and directory listings; • Aim to provide individuals with privacy when using electronic devices and keep communications secure.
Freedom of Information (Scotland) Act 2002 (FOISA)	• Supports and encourages the disclosure of information. • Under FOISA, anyone who requests information from a Scottish public authority that holds it, is entitled to be given it by the authority (subject to a limited number of exemptions) within a set timescale. • Enforced and promoted by the Scottish Information Commissioner (SIC).
Environmental Information (Scotland) Regulations 2004 (EIRs)	• Originate from a European Directive on access to environmental regulation. • They give everyone the right to ask for environmental information held by a Scottish public authority (subject to a limited number of exceptions) within a set timescale. • Enforced and promoted by the SIC.
The Pupils' Educational Records (Scotland) Regulations 2003	• Under these regulations, parents and guardians can request copies of their child's educational records (these requests are fulfilled by the school that holds the information); • These regulations apply to records relating to school pupils, past and present. The regulations stipulate that educational records must be retained for a period of five years following the child having ceased receiving school education.
The INSPIRE (Scotland) Regulations 2009	• Originate from a European Directive. • These regulations require Scottish public authorities to make spatial datasets available.

	• The regulations are enforced and promoted in Scotland by the SIC.
Public Records (Scotland) Act 2011 (PRSA)	• Governs the management of public records; • Named authorities must create a 15 point Records Management Plan (RMP) in line with the Model Plan created by the Keeper of the Records of Scotland ('the Keeper'); • Authorities can undergo optional review of their RMPs on an annual basis, by utilising the 'Progress Update Review Mechanism'. Active engagement provides National Records Scotland (NRS) greater assurances regarding the authority's compliance.

Appendix 2 – Access to Information Key Performance Indicators

EDUCATION RESOURCES & COMMUNITIES (Alison Morris) 2022/25

Generated on: 29 March 2023

PI Status	
	Alert
	Warning
	OK
	Unknown
	Data Only

Long Term Trends	
	Improving
	No Change
	Getting Worse

Short Term Trends	
	Improving
	No Change
	Getting Worse

Cannot group these rows by Theme

All Indicators

Code	Code	Short Name	Current Target	2020/21	2021/22	2022/23	Q4 2021/22	Q1 2022/23	Q2 2022/23	Q3 2022/23	Q4 2022/23	Latest Note	Short Term Trend Arrow	Status
				Value	Value	Value	Value	Value	Value	Value	Value			
CE015	Local(b)	Freedom of Information - Percentage of requests replied to within twenty working days	95%	89.8%	92%		85.2%	85.8%	85.5%	84.6%	90.5%	Please note that this figure does not include all requests received in this Quarter as those received after 27/03/2023 are not due until after the date this data is requested (20 requests)		
CE015a	MI	Freedom of Information Requests - Number received	Data Only	N/A	1,006	575	273	264		311	346	8 requests are still outstanding		
CE015b	MI	Freedom of Information Requests - Number responded to within 20 working days	Data Only	N/A	874	491	209	228	326	263	313			
CE015c	MI	Freedom of Information Requests - Number of exemptions	Data Only	N/A	N/A	N/A								
CE015d	MI	Freedom of Information Requests - Hours taken to answer	Data Only	N/A	N/A	N/A								
CE015e	MI	Freedom of Information requests - Average time taken to answer	Data Only	N/A	N/A	N/A								
CE016a	MI	Environmental Information Requests (EIR) - Number received	Data Only	N/A	59	11	5	4		7	17			
CE016b	MI	Environmental Information Requests (EIR) - Number responded to within timescale	Data Only	N/A	48	10	0	4		6	15			
CE016c	MI	Environmental Information Requests (EIR) - Number of exemptions	Data Only	N/A	N/A	0	N/A			0				

Code	Code	Short Name	Current Target	2020/21	2021/22	2022/23	Q4 2021/22	Q1 2022/23	Q2 2022/23	Q3 2022/23	Q4 2022/23	Latest Note	Short Term Trend Arrow	Status
				Value	Value	Value	Value	Value	Value	Value	Value			
CE016d	MI	Environmental Information Requests (EIR) - Hours taken to answer	Data Only	N/A			N/A							
CE016e	MI	Environmental Information Requests (EIR) - Average time taken to answer	Data Only	N/A			N/A							
CE017a	MI	Subject Access Requests (SAR) - Number received	Data Only	N/A	53	23	17	9		14	25	+ 4 suspended		
CE017b	MI	Subject Access Requests (SAR) - Number responded to within timescale	Data Only	N/A	N/A	12	N/A			12	20			
CE017c	MI	Subject Access Requests (SAR) - Number of exemptions	Data Only	N/A	N/A	0	N/A			0				
CE017d	MI	Subject Access Requests (SAR) - Hours taken to answer	Data Only	N/A	N/A		N/A				85.7hrs			
CE017e	MI	Subject Access Requests (SAR) - Average time taken to answer	Data Only	N/A	N/A		N/A				3.1hrs			
CE037	Local(b)	Data Protection - Percentage of requests responded to within 30 calendar days	95%	89.5%	86.5%		75%	77.8%	81.8%	85.7%	80%			

Appendix 3 – Links

Legislation

- Data Protection Act (DPA) 2018
  https://www.legislation.gov.uk/ukpga/2018/12/contents
- Data Protection and Digital Information (No.2) Bill
  https://bills.parliament.uk/bills/3430
- The Government has published Keeling Schedules to show the changes that will be made to UK GDPR, the Data Protection Act 2018 and the Privacy and Electronic Communications Regulations 2003 by the Data Protection and Digital Information (No. 2) Bill
  https://www.gov.uk/government/publications/data-protection-and-digital-information-bill-impact-assessments
- Freedom of Information (Scotland) Act 2002
  https://www.legislation.gov.uk/asp/2002/13/contents
- INSPIRE (Scotland) Regulations 2009
  https://www.legislation.gov.uk/ssi/2009/440/contents/made
- Public Records (Scotland) Act 2011
  https://www.legislation.gov.uk/asp/2011/12/contents
- The Environmental Information (Scotland) Regulations 2004
  https://www.legislation.gov.uk/ssi/2004/520/contents
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
  https://www.legislation.gov.uk/uksi/2003/2426
- The Pupils' Educational Records (Scotland) Regulations 2003
  http://www.legislation.gov.uk/ssi/2003/581/contents/made
- UK GDPR (the General Data Protection Regulation (as defined in the DPA 2018) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019
  https://www.legislation.gov.uk/eur/2016/679/contents#top

Interchange and Relevant Websites

- Information Governance Interchange Page (incl. RM, DP and Access to Information)
  http://interchange.moray.gov.uk/int_standard/Page_132356.html
- Moray Council Information Management webpages (incl. DP, FOIs and RM)
  http://www.moray.gov.uk/moray_standard/page_41220.html
- National Records of Scotland
  https://www.nrscotland.gov.uk/
- Scottish Information Commissioner
  https://www.itspublicknowledge.info/
- The Information Commissioner's Office
  https://ico.org.uk/