Information Governance Policy

Publication code: IG-1222-001.2

Publication date	March 2025
Version number	1.3
Author's initials	CR
Job title	Information Governance co-ordinator
Responsibility for this document	Senior Information Risk Owner
Review date	Two years from publish date

First version agreed by Executive Group.

Changes:

Date update front cover, footer dates

1. Introduction

The Care Inspectorate is a scrutiny body which supports improvement. That means we look at the Quality of Care in Scotland to ensure it meets high standards.

Our vision is that everyone experiences safe, high- quality care that meets their needs, rights and choices.

Our main business functions include:

- Corporate and Customer Services, including Finance, Estates, HR, Legal Services, Information and Communication Technologies (ICT),
- Scrutiny and Assurance, including Registration, Inspection, Enforcement, Complaints,
- Strategy and Improvement, including Communications, Information Governance (IG), Intelligence, Organisational Workforce Development (OWD), Policy, Strategy and Improvement, Professional Practice.

Information is a key asset for the Care Inspectorate and needs to be valued. Access to reliable, relevant, secure, accurate and timely information underpins all the actions we take and decisions we make when carrying out the work of the Care Inspectorate.

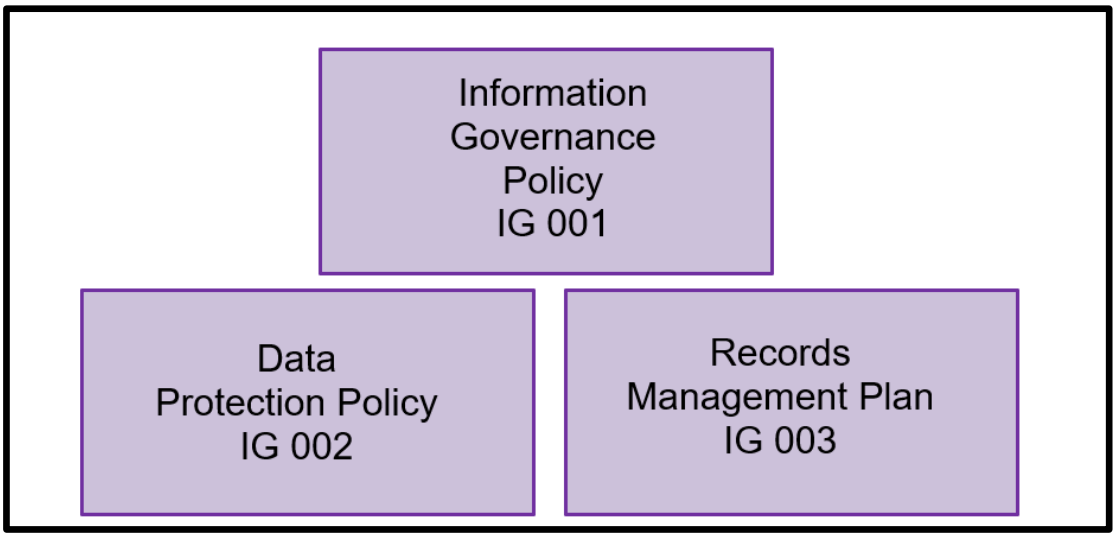
Ultimately, it enables intelligence-led scrutiny and assurance of regulated care services in Scotland, helping us deliver our vision that everyone experiences safe, high-quality care that meets their needs, rights, and choices.

This document sets out the Care Inspectorate's overarching Information Governance (IG) policy and explains how we as an organisation manage our records in accordance with our *Records Management Plan*[1]. It is crucial that we manage our information assets to meet the strategic, operational and legal requirements of the Care Inspectorate to maximise its value for the organisation and its stakeholders and to stop it becoming a liability and a risk. Good IG provides that assurance.

The commitments required to achieve this governance fall under two main categories which each have policy area-specific elements: Data Protection and Records Management. The hierarchy is shown below in Figure 1 and the policy area specific elements are listed at Annex 1.

Figure1: Policy Structure

[1] IG003 Records Management Plan



2. Responsibilities

2.1 All Care Inspectorate Colleagues

All Care Inspectorate colleagues have a professional responsibility to keep accurate and timely records about their work and store them in the right repositories.

Records could be anything written, photographed, typed, copied or recorded in the course of your work for the Care Inspectorate, whether in relation to a care service, a local authority, a local partnership, or persons involved with these services, or for the management and administration of the organisation. These include notes, reports, emails, letters, images, audio-visual recordings, copies of documents and evidence.

The way information is recorded, stored, and shared is crucial to effective communication, accountability and evidence-based decision making. Colleagues will rely on these records at key decision points, especially during enforcement procedures or major inquiries relating to case work. All staff are accountable, whatever their level or area of responsibility to comply with IG policy.

Records should be created using the devices provided by the organisation, using corporate templates where appropriate, and stored in the appropriate files or folders within the Care Inspectorate Office 365 environment, activity specific application or hard copy case file at the earliest opportunity. They must not be retained on non-Care Inspectorate devices, within OneDrive or local drives on laptops or surface pros, or in hard copy at home for longer than necessary.

You must only record what is necessary and relevant to our organisational purposes. Documents that are not required and additional to our purposes and received from a person or service should be returned to those individuals or services directly. Records must be created at the time of the events they refer to or as soon as possible afterwards. All physical or digital documents must adhere to the Naming Conventions policy[2]. Records must be accurate and recorded in such a way that the meaning is clear and unambiguous.

2.2 Executive Group.

The Executive Group has overall responsibility for ensuring that records are created and

[2] IG003 Naming Conventions

managed by their departments and functions to meet the needs of the Care Inspectorate and in line with organisational policy.

2.3 Senior Information Risk Owner (SIRO)

The Executive Director of IT, Transformation and Digital is the Care Inspectorate's SIRO. The SIRO is the senior officer responsible for the management of the Care Inspectorate's records under section 1(2)(a) of the Public Records (Scotland) Act, 2011. The SIRO is also responsible for the management of Information Risk.

2.4 Information Asset Owners (IAOs)

IAOs have overall responsibility to ensure that records within their Directorate are managed according to statutory responsibilities and Care Inspectorate policies. They are also responsible for identifying and managing information risk within their functional area.

2.5 Business Process Owners (BPOs)

BPO's are the gatekeepers for information and risk management – BPOs can be any grade but they understand a process or activity and are accountable to the Information Asset Owners for identifying and managing risk

2.6 Line Managers

All line managers must ensure that this policy and all associated Records Management and Data Protection policies, procedures and guidance are understood by all staff within their business units and that these are incorporated into routine administrative practices. It is a line manager's responsibility to make sure that their staff have had adequate training in all aspects of IG, take training opportunities when they are available and are given the time to do so.

2.7 Information Governance

The IG team are responsible for the development, updating, dissemination and operational delivery of the Information Governance, Records Management and Data Protection policies, procedures, guidance, awareness, and training.

2.8 IG Lead

The IG Lead is identified as holding operational responsibility for records management and has appropriate corporate responsibility, access to resources and skills. As required in Section 1(2)(a)(ii) of the Act this is the person responsible for ensuring the authority complies with its records management plan and provides the first point of contact for the Keeper on records management issues.

3. Records Management

3.1 Records Management Policy Suite

The Records Management Policy Suite contains policies, associated procedures and guidance that when followed, ensure that all records held by the Care Inspectorate are effectively managed throughout their life cycle.

In order for the value of Care Inspectorate records to be maintained and assured, they need to be managed efficiently, transparently and consistently from the point they are created or received, through maintenance and use, to the time they are destroyed or permanently preserved as archival records as shown in Figure 2.

The capture of good records, in the right repositories, reduces the time and resource needed to deliver our strategic priorities and prevents costly duplication of work.

Figure 2: Records Lifecycle

3.11_Creation and capture

The Care Inspectorate is the owner or Data Controller of all Care Inspectorate records, including those created by Board members, employees, contractors, or consultants.

Records must be created and captured in the appropriate recordkeeping systems.

Records must be adequate for the Care Inspectorate business they support.

To achieve this, the Care Inspectorate is committed to meeting the following principles of good records management as defined by the National Records of Scotland:

- **Authentic** – it must be possible to prove that records are what they purport to be and who created them, by keeping a record of their management through time. Where information is later added to an existing document within a record, the added information must be signed and dated. With electronic records, changes and additions must be identifiable through audit trails.
- **Accurate** – records must accurately reflect the transactions that they document.
- **Accessible** – records must be readily available when needed.
- **Secure** – records must be securely maintained to prevent unauthorised access, alteration,

damage or removal. They must be stored in a secure environment

- **Comprehensive** – records must document the complete range of an organisation's business.
- **Compliant** – records must comply with any record keeping requirements resulting from legislation, audit rules and other relevant regulations.
- **Effective** – records must be maintained for specific purposes and the information contained in them must meet those purposes.

All records must be titled and referenced as per the Naming Conventions[3] procedure and consistent and relevant to the business activity to ensure that they can be easily retrieved, understood and managed.

Care Inspectorate records should be created in fixed formats wherever possible to maintain their integrity over time.

Staff should use the Government Security Classification (GSC) procedure[4], identifying OFFICIAL information and labelling SENSITIVE data as it is created. This will assist the Care Inspectorate when processing information by ensuring that sensitive information is being secured and shared in the right way and in accordance with our privacy notice.

All records repositories must reflect the Metadata Standard[5] and this must be built into the requirements for any new (developed/bespoke or Commercial Off The Shelf (COTS)) records repository.

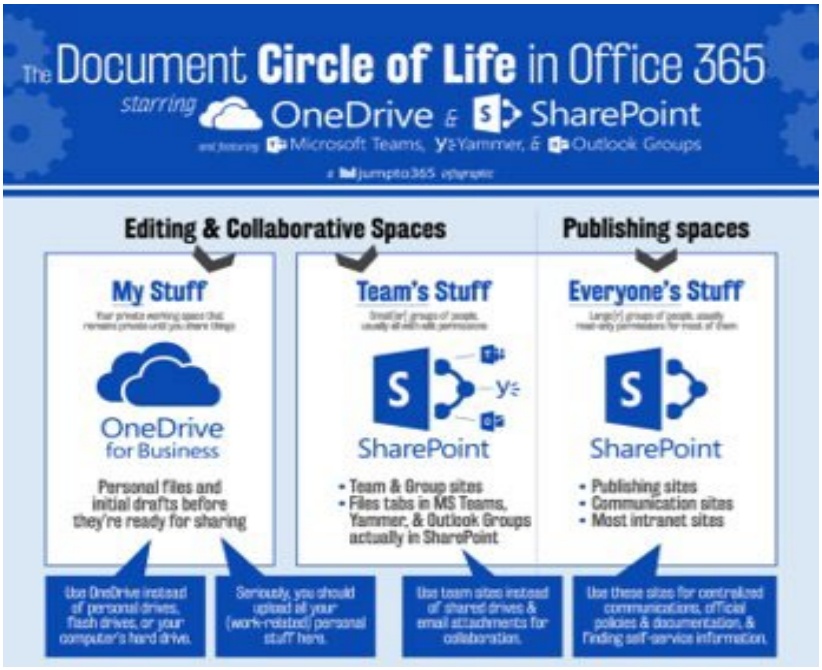
3.12_Storage and retrieval

Care Inspectorate records must be adequately protected and stored securely to prevent unauthorised access.

Digital records outside of authorised applications must be stored within the Office 365 suite which has been configured in line with the Care Inspectorate's Business Classification Scheme (BCS) and related information architecture standards, and in line with the policies identified in Figure 3.

Figure3: Office 365

[3] IG003 Naming Conventions
[4] IG002 Government Security Classification
[5] IG003 Metadata Standard



The Care Inspectorate has adopted a digital-by-default approach. However, where master records need to be retained in physical format, they should be stored within the agreed formal filing structure that conforms to the Care Inspectorate's BCS and related information architecture standards as identified in our hard copy file and retrieval policies[6].

Physical records must be archived in line with the published Care Inspectorate Information Retention and Disposal Schedule[7] and archived with our offsite provider. Files must be appropriately listed with relevant record retention rules and labelling requirements detailed.

Complying with the Records Management policies also ensures that we can easily find information within the statutory deadlines when people exercise their rights. Under Data Protection legislation Data Subjects have the right to access the information that the Care Inspectorate holds about them. Under the Freedom of Information (Scotland) Act 2002 we are required to access information held relating to Care Inspectorate statutory work and functions, see Annex 2 for the statutory framework from within which we must operate.

3.13 _Management

Care Inspectorate records must have access controls and audit logging in place that are appropriate to the sensitivity and risk of their content. Care Inspectorate records must remain accessible and usable for as long as they are required to be retained under the Care Inspectorate's Retention Schedule.

All records created during your work are Care Inspectorate records and must be available to colleagues whilst being mindful of the sensitivity.

All Care Inspectorate records must be recorded on the Information Asset Register (IAR) under a relevant classification.

[6] IG003 Hard Copy Records Management.
[7] IG003 Review and Retention & IG003.3a Retention Schedule

Care Inspectorate records that are vital to the continuity of Care Inspectorate business must be identified as Vital Records by the business areas responsible for them and recorded on the Information Asset Register as such, see role of the information asset owner at 2.4.

Care Inspectorate records must not be distributed or copied unnecessarily.

3.14_Digital preservation

Digital Care Inspectorate records that are required for long term (ten years or more) retention or archival transfer to the National Records of Scotland should be kept in robust file formats identified in the Digital Preservation Strategy.

3.15_Disposal

No Care Inspectorate record may be destroyed without appropriate authorisation and due regard to both legal obligations and the Care Inspectorate's Retention Schedule.

All destructions of Care Inspectorate records must be logged by the disposing business unit where indicated in the Care Inspectorate's Retention Schedule.

Care Inspectorate records must be destroyed securely, in compliance with the Care Inspectorate's procedures.

4. Data Protection

4.1 Data Protection Policy Suite

As the scrutiny and improvement body for social care and social work services across Scotland, the Care Inspectorate has powers under Part 5 of the Public Services Reform (Scotland) Act 2010 to collect and process personal information about people who provide, manage and work for care services and people experiencing care. The Care Inspectorate also collects and processes types of personal data about a variety of other individuals as part of its day to day operations. These include current, past and prospective employees, volunteers, suppliers and others with whom it communicates.

To protect the privacy of those individuals, the Care Inspectorate is required to comply with two pieces of legislation; the Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR). The DPA sets out the framework for data protection law and tailors how the GDPR applies in the UK, they sit alongside each other.

The GDPR establishes a framework of rights and duties which balance the need of organisations to collect and process Personal Data for clearly defined purposes with the right of the individuals to confidentiality. These individuals are known as Data Subjects.

Compliance with the GDPR and related privacy law is not just a legal obligation. The Care Inspectorate regards the lawful and correct treatment of personal information as of vital importance to maintaining trusted and positive working relationships with the various groups of individuals whose personal data the Care Inspectorate holds and to ethical and successful business practice. The Privacy Notice[8] published on our website explains how and why we process personal data.

4.1.1 Information Security & Risk

The Records Management Policy looks at the principles for good record keeping such as the systems to use, what to record, the purpose for collection, confidentiality, security of records as well as access and disclosure.

The Data Protection Policy includes our instruction on how to make sure we are legally compliant with the security principle; we must protect all our information appropriately and in line with agreed business practice and operational policy. We must have in place organisational and technical measures that ensure:

- The confidentiality of information that is personally, commercially, or operationally sensitive
- The integrity of our information to ensure that it can be trusted to be accurate, current, and complete with proper naming conventions.
- The availability of our information is to ensure that it can be accessed by the right people at the right time in the right place.

The identification and consideration of information risks and IG requirements are undertaken as an integral part of organisational and technological change and risk assessed, as appropriate, in conjunction with relevant stakeholders.

[8] IG002 Care Inspectorate Privacy Notice

The information or records that the Care Inspectorate collect through our regulatory work are Information Assets (IAs). An IA is a body of information, defined and managed as a single unit so it can be understood, shared, protected, and exploited effectively.

Each asset must have an IAO. This is the Care Inspectorate manager responsible for ensuring that the risks to, and the opportunities for the asset, are monitored and are listed on the IAR. The IAO doesn't need to be the creator or the primary user of the asset, but they must understand its value to the organisation.

- IAs need to be understood, shared, protected, and exploited effectively.

- IAs have a recognisable and manageable value, risk, content and lifecycle as per our retention schedule.

IAOs must review the assets they are responsible for to keep the IAR relevant. The SIRO is the owner of the IAR and will instruct IAOs on maintenance requirements[9].

The Care Inspectorate ensures that records and IAs remain safe by adopting quality assurance measures that are best practice and by completing risk-based assessments before any technical business change[10].

- Our processes use ISO/IEC 27001 and National Cyber Security Centres (NCSC) Software as Service security principles for guidance in defining an asset-based risk-based approach to information security.
- The risk assessment process is triggered before each new digital service.
- We ensure that repeated risk assessments produce "consistent, valid and
- comparable results".
- ICT Service Team retain documented information about its risk assessment process so that it can demonstrate compliance with these requirements.

4.1.2 Data Breaches

All staff are responsible for ensuring that:

- any personal data that they hold, no matter the format, is held securely

- personal data is not disclosed either orally or in writing, accidentally or otherwise, to any unauthorised third party.

We have robust and documented Data Breach procedures and controls for identifying, investigating, reviewing, and reporting any data breaches or near misses through the "One Trust platform" via a link on our intranet page[11]. All staff must report breaches in a timely manner and if the threshold is reached, IG must report data breaches within 72 hours to the Information Commissioner's Office (ICO).

[9] IG002 Information Risk Handbook (under development)
[10] ICT policies are in draft – awaiting publication.
[11] IG002 Data Breach (process if updating)

4.1.3 Privacy and Data Protection Impact Assessments (DPIAs)

The UK GDPR and Data Protection Act 2018 require that appropriate technical and organisational measures are taken to implement the data protection principles and safeguard individual's rights. This is known as 'data protection by design and by default' previously known as Privacy by Design.

This means that the Care Inspectorate is required to integrate data protection into all processing activities and business practices, from the design right through the life cycle to decommissioning.

A DPIA is a statutory process that helps to identify privacy risks associated with organisational change and ensures lawful practice is maintained throughout the change process from planning and implementation to business-as-usual. The purpose of the DPIA is to ensure that privacy risks are minimised while allowing the aims of the project to be met whenever possible. It achieves this by taking proactive and preventative rather than reactive and remedial measures to manage privacy risks.

A DPIA enables privacy risks to be identified and mitigated at an early stage by analysing how the proposed uses of personal information will work in practice. It is a consultative process and involves engagement with people who will be working on, or affected by, the project.

All staff must, prior to any new initiative, process, or project carry out a DPIA screening assessment through the "One Trust" platform by contacting the IG team followed by a DPIA if potential privacy risks are identified. A screening assessment must also be completed if there is a wholesale change to an existing process, or a new procurement.[12]

[12] IG002 Data Protection Impact Assessment (DPIA); IG002 Data Protection Impact Assessment (DPIA) Screening Form ; IG002 Data Protection Impact Assessment (DPIA) Form

5. Conclusion

All Care Inspectorate staff have a responsibility to comply with IG policy and some staff have specific responsibilities which are summarised in Section 2.

All Care Inspectorate staff have a professional responsibility to keep accurate and timely records about their work. All staff also have a responsibility to identify and mitigate information risk.

The way you record and share information is crucial to effective communication, accountability and evidence-based decision making.

Colleagues will rely on your records at key decision points and all information you generate must therefore be available to colleagues when required and in accordance with the GSC Policy.

The IG team are available for any help and support in complying with the policies, and they will be performing compliance checks to make sure that individuals, teams and departments are practicing good Information Governance.

This policy will be reviewed bi-annually or more frequently if required by significant changes in legislation, regulation or business practice. It will be reviewed by the IG Team and presented to the Care Inspectorate Executive Group for approval, in line with the Care Inspectorate's Policy Framework.

Annex 1 - Policy Structure Overview

1. Information Governance Policy:

IG001 Information Governance Policy
IG001.3 Freedom of Information (Scotland) Policy
IG001.2 Information Governance Enquiries Procedure

2. Data Protection Policy:

IG002 Data Protection Policy

2.1 Data Protection Procedures:

IG002 Care Inspectorate Privacy Notice[13]
IG002 Data Protection Impact Assessment (DPIA) Procedure
IG002 DPIA Screening Form
IG002 DPIA Form
IG002 Data Breach Procedure
IG002 This should be sensitivity label procedure but isn't a stand-alone document yet I don't think?
IG002 Government Security Classification
IG002 Information Risk Handbook

3. Records Management Policy:

IG-003 Records Management Plan

3.1 Records Management Procedures:

IG003.1 Records Management Action Plan
IG003.2 Metadata Standard
IG0003.3 Naming Conventions
IG-003.4 Review and Retention
IG003.4a Retention Schedule
IG003.5 Hard Copy Records Management
IG003.5a Disposal Form
0003.6a O365 One Drive
0003.6b O365 SharePoint
0003.6c O365 Sharing
0003.6d O365 Teams

[13] https://www.careinspectorate.com/index.php/core-privacy-notice

Annex 2 Legislation and Regulation Relating to Information Governance in the Care Inspectorate:

The Care Inspectorate was established under section 44(1) of the Public Services Reform (Scotland) Act 2010 as an independent body responsible for the scrutiny and improvement of care, social work and child protection. The role and functions of the Care Inspectorate are set out in the Public Services Reform (Scotland) Act 2010 and the Adults with Incapacity (Scotland) Act 2000 (Part 4 only).

Below is a list of the main legislation which impacts upon Information Governance.

Statute or Regulation	Summary of Impact
1. Public Services Reform (Scotland) Act 2010 https://www.legislation.gov.uk/asp/2010/8/contents • ***Our predecessor, the Care Commission drew its powers from the Regulation of Care (Scotland) Act 2001*** • *http://www.legislation.gov.uk/asp/2001/8/section/1*	**1.1 The Care Inspectorate draws its power from this Act.** The overarching aim of the Act is to simplify and improve Scotland's public services by: Helping to simplify and improve Scotland's complex landscape of public bodies by dissolving some smaller bodies and merging others with similar functions Providing a legislative process for Parliament to make further necessary structural changes to public bodies Providing a power to remove and reduce unnecessary burdens on businesses and the wider economy Establishing more effective structures for the improvement and scrutiny of health, social care and social work Ensuring improvement and scrutiny bodies work together and are focused on the user **1.2 Section 53(6) outlines our statutory power to require a social service to supply us with any information relating to the service that is necessary for us to carry out our statutory functions.**
2. Scottish Statutory Instrument No 185 **The Public Services Reform (Social Services (Social Services Inspections) (Scotland) Regulations 2011**	2.1 The Scottish Ministers made the following Regulations in exercise of the powers conferred by section 58(1) of the Public Services Reform (Scotland) Act 2010(1) and all other powers enabling them to do so. **2.2 Paragraph 5 outlines in more detail our power to acquire information.**

http://www.legislation.gov.uk/ssi/2011/185/made	**2.3 Paragraph 9 outlines our specific obligations in relation to the disposal of personal records that were obtained for the purposes of an inspection.** **2.4 Paragraph 10 details our powers in relation to sharing information that we obtained for the purpose of an inspection.**
3. Public Records (Scotland) Act 2011 https://www.legislation.gov.uk/asp/2011/12/contents	3.1 Under the Public Records (Scotland) Act 2011 (the Act) Scottish public authorities must produce and submit a records management plan (RMP) setting out proper arrangements for the management of an authority's public records to the Keeper of the Records of Scotland (the Keeper) for his agreement under section 1 of the Act.
4. Freedom of Information (Scotland) Act 2002 http://www.legislation.gov.uk/asp/2002/13/contents	The Freedom of Information (Scotland) Act 2002 (FOI(S)A) is an Act of the Scottish Parliament which gives everyone the right to ask for any information held by a Scottish public authority. This right is subject to certain conditions and exemptions, which are set out in the Act. FOI(S)A is enforced and promoted by the Scottish Information Commissioner **In summary, FOI(S)A requires the Care Inspectorate to either make available the information requested by an applicant, or to explain why the information in not being made available.** **Scottish Ministers, in consultation with the Scottish Information Commissioner, have produced 'best practice' guidance for Scottish public authorities on discharging functions under FOI(S)A.** It stresses the best practice to be followed in providing advice and assistance to requesters and promotes the importance of proactively publishing information. Public authorities subject to FOI(S)A must also have a Publication Scheme which sets out the information that they will routinely publish. The Care Inspectorate has adopted the Model Publication Scheme, which was produced by the Scottish Information Commissioner.
5. Data Protection Act 2018 http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf	Member States can introduce exemptions from the UK GDPR's transparency obligations and individual rights, but only where the restriction respects the essence of the individual's fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard: national security; defense; public security;

	the prevention, investigation, detection or prosecution of criminal offences; other important public interests, in particular economic or financial interests, including budgetary and taxation matters, public health and security; the protection of judicial independence and proceedings; breaches of ethics in regulated professions; monitoring, inspection or regulatory functions connected to the exercise of official authority regarding security, defence, other important public interests or crime/ethics prevention; the protection of the individual, or the rights and freedoms of others; or the enforcement of civil law matters. The GDPR provides the following rights for individuals: The right to be informed. The right of access. The right to rectification. The right to erasure. The right to restrict processing. The right to data portability. The right to object. Rights in relation to automated decision making and profiling. The Data Protection Act 2018 is the UK's implementation of the GDPR. Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They state that data must be: a) processed lawfully, fairly and in a transparent manner in relation to individuals; b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes…; c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; d) accurate and, where necessary, kept up to date…; e) kept…for no longer than is necessary for the purposes for which the personal data are processed; f) processed in a manner that ensures appropriate security of the personal data… **Law enforcement data processing provisions** Part 3 of the Act strengthens the rights of data subjects whilst enabling The Care inspectorate to restrict these rights where this is necessary to, amongst other things, avoid prejudicing the

	prevention, detection, investigation or prosecution of criminal offences, for example by revealing to a person that they are under investigation. Places restrictions on the rights of the data subject, but only where necessary and proportionate in order to: a) avoid obstructing an investigation or enquiry; b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties; c) protect public security; d) protect national security; and e) protect the rights and freedoms of others There are likely to be three circumstances when we may need to share personal data with a law enforcement authority to enable us to carry out our functions: • where we want to proactively share personal data; for example, if we want to report a crime to the police and provide relevant personal data we hold; • where we receive a request from a law enforcement authority for personal data held; for example, the police may request personal data from us to help them investigate a crime; or a sudden death • where a court order or another legal obligation compels us to share personal data with a law enforcement authority.
6. The Re-use of Public Sector Information Regulations 2015 http://www.legislation.gov.uk/uksi/2015/1415/contents/made	6.1 Re-use Care Inspectorate documents, information or resources are covered by the Re-use of Public Sector Information Regulations .
7. Environmental Information (Scotland) Regulations 2004 http://www.legislation.gov.uk/ssi/2004/520/contents/made	The Environmental Information (Scotland) Regulations 2004 ('the EIRs') are based on European Directive 2003/4/EC ('the Directive'). They give the public rights of access to environmental information held by Scottish public authorities. The EIRs require Scottish public authorities to: • Actively disseminate information, particularly by electronic means **(regulation 4(1));** • Make environmental information available to any person who requests it within 20 working days or, in exceptional cases where the request is both

	voluminous and complex, within 40 working days **(regulation 5(1)** and **regulation 7(1));** • Publish a schedule of charges and information on the circumstances in which a fee may be charged, waived or required to be paid in advance **(regulation 8(8));** • Provide advice and assistance to someone who has made, or wishes to make, a request for environmental information **(regulation 9);** • Refuse environmental information only in accordance with the limited exceptions available, giving reasons and details of the mechanisms for review and appeal **(regulations 10, 11, 13, 16 and 17);** • Transfer requests for environmental information if they do not hold the information but believe another authority does **(regulation 14);** • Where requested, carry out a review of a decision not to make environmental information available **(regulation 16).**
European Convention on Human Rights (ECHR) **https://www.echr.coe.int/Documents/Convention_ENG.pdf**	The European Convention on Human Rights (ECHR) protects the human rights of people in countries that belong to the Council of Europe. **Article 8 – Right to respect for private and family life** • The right to a private life protects your dignity and autonomy. It covers both public and private interactions and includes respect for your private and confidential information, particularly the storing and sharing of data.

Additional Legislation - Care Inspectorate

A list of the additional legislation which may impact on the scrutiny and assurance work of the Care Inspectorate, is published on the Care Inspectorate Hub.