Data Protection Policy

Publication code:

Publication date	June 2018
Version number	2.0
Author's initials	HJ
Job title	IG Consultant
Responsibility for this document	Senior Information Risk Officer
Review date	June 2020
Key changes made since last version of document	
This document replaces the Data Protection Policy v1-0 IG-1014-010	

INTRODUCTION

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 the General Data Protection Regulation (GDPR). 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 legislation is not just a statutory 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.

PURPOSE

The purpose of this policy and related procedures and guidance is:

- to set out the Care Inspectorate's obligations under the GDPR for fair, lawful and transparent processing of personal data in the information created and received in the course of its activities

- to demonstrate its commitment to, and compliance with, the GDPR and related legislation and standards that govern the privacy of individuals with whom the Care Inspectorate has a relationship

- to ensure that individuals feel secure when providing us with personal information and know that it will be handled in accordance with their rights under the data protection law.

SCOPE

The GDPR relates to the processing of personal data. Personal data is factual information that both identifies and relates to a living individual and includes any expression of opinion about the individual.

The GDPR classifies some types of personal data as "special category" data to which stricter conditions apply. This includes personal data concerning racial or ethnic origin, political or religious beliefs, trade union membership, physical or mental health, sexual orientation and criminal records.

The policy is applicable to all Care Inspectorate employees, volunteers, suppliers and other organisations working for or on behalf of the Care Inspectorate.

The policy applies to all personal data regardless of format or medium, including paper, electronic, audio, visual, and photographic.

POLICY COMMITMENT

In order to fulfil its obligations under the GDPR, the Care Inspectorate is committed to complying with the six data protection principles.

Article 5.1 of the GDPR requires that personal data shall 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; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial 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; 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;

e) 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 subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

f) 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.

The Care Inspectorate is also committed to complying the “accountability” principle set out under Article 5.2 which states that:

“the controller shall be responsible for, and be able to demonstrate, compliance with the principles”

To comply with these principles, the Care Inspectorate is committed to the following policy statements and to the development and maintenance of related procedures, processes and systems to fulfil that commitment.

THE RIGHTS OF DATA SUBJECTS

The Care Inspectorate will ensure that people about whom it holds information can exercise their rights under the Regulation.

The GDPR provides the following rights for data subjects:

The right to be informed

The Care Inspectorate only collects and processes personal information where it is fair and lawful to do so to exercise its statutory powers, fulfil operational needs or to comply with any other legal requirements.

We will inform data subjects of processing activities and provide them with required statutory information at the time data is collected, or when we first contact the data subject in relation to the personal data they have provided.

We will do this through the use of explicit privacy statements whenever data is gathered, for example on a form, and provide easy access to full privacy notices that are concise and transparent and are written in clear and plain language. These notices will outline the purpose for which it will be used and the legal processing condition, who it will be shared with, how it will be securely retained, how long it will be kept for and how individuals may access it.

The Care Inspectorate will seek explicit consent from its data subjects when collecting special categories of information, collecting personal data for unexpected or potentially objectionable purposes, processing information in a way which may significantly affect an individual, sharing information with another organisation which would be unexpected, except where statutory exemptions apply, for example when exercising our statutory powers under Part 5 of the Public Services Reform (Scotland) Act 2010.

The right of access

Subject access requests are requests to the Care Inspectorate made by the data subject for access to the personal information we hold about them. In some cases subject access requests are made by a third party on that person's behalf, for example by

- a parent or guardian on behalf of a young child (under 12 years of age)
- a representative on behalf of an adult with incapacity
- a solicitor on behalf of a client.

We will take reasonable steps to make sure that the person making the subject access request is who they say they are. If someone is making a request on behalf of a third party, we will check that they have the authority to make that request.

Requests for access to personal data, other than those falling within routine business, should be addressed in writing or email to the Data Protection Officer, ideally using the subject access request form available on the Care Inspectorate website, or in hard copy, on request.

We aim to comply with requests for access to personal information within 28 calendar days from data of submission of a validated request, unless there is a good reason for delay. In such cases, the reason for delay will be explained, in writing, to the Data Subject making the request.

The right to rectification

All staff working with personal data will ensure data remains as accurate and up-to-date as possible in line with our data quality policy and procedures.

Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.

We will make it easy for Data Subjects to update the personal data the Care Inspectorate holds about them.

All employees are responsible for:

- checking that any personal data that they provide, in connection with their employment, are accurate and up to date;
- informing the Human Resources Department of any changes to their personal data they have provided, i.e. change of address and of any errors in their Personal Data.

The right to erasure

The Care Inspectorate will retain personal data only for as long as it is needed and ensure its secure disposal at the end of this period through the maintenance and application of our information retention schedule, information life-cycle management procedures and confidential destruction procedures.

The right to erasure does not provide an absolute right to be forgotten. Data subjects have the right to have personal data erased or prevent further processing under certain conditions:

- where the personal data is no longer required for the purpose it was originally collected for.

- when the data subject withdraws consent, where consent was the legal processing condition.
- when the data subject objects to processing and there are no overriding, legal reasons for continuing to process the personal data.
- where the processing was unlawful to begin with.
- where the personal data has to be erased in order to comply with a legal obligation.
- where the personal data is processed in relation to supplying ‘information society services’ to children.

The Care Inspectorate can refuse the right of erasure under the following circumstances:

- when complying with a legal obligation for the performance of a public task or exercise of official authority.
- for public health purposes in the public interest.
- the exercise or defence of legal claims.
- when archiving in the public interest, scientific or historical research or statistical purposes.
- when exercising the right of freedom of information or expression.

The right to restrict processing

Data subjects have the right to restrict, block or supress the processing of personal data. When processing is restricted, the Care Inspectorate is permitted to retain the personal data but no further processing must take place.

The Care Inspectorate will restrict processing in the following conditions.

- Where the accuracy of the personal data is contested by the data subject. Processing will be restricted until the accuracy of the Personal Data has been verified.
- Where the processing has been objected to by the Data Subject and the processing was on the basis of performance of a public task. Processing will be restricted while we considers the whether the legitimate grounds override the rights of the data subject.

- When the processing was unlawful and the data subject requests restriction rather than erasure.
- When we no longer require the personal data but the data subject required the personal data to be retained to establish, exercise or defend a legal claim.

The right of data portability

Data portability allows a data subject to obtain their personal data to reuse across different services. It allows the moving, copying or transferring of their personal data from one IT system to another in a safe and secure manner. The right of data portability only applies:

- to personal data a Data Subject has provided to the Care Inspectorate
- where the legal processing condition is consent or for the performance of a contract
- when the processing is carried out by automated means.

The right to object

Data subjects have the right to object to processing based on legitimate interests, performance of a task in the public interest, direct marketing, profiling and for the purposes of historical or scientific research and statistics. The Care Inspectorate will stop processing unless

- the Care Inspectorate can demonstrate compelling legitimate grounds which override the rights of the data subject
- the processing is for the establishment, exercise or defence of legal claims.

Rights related to automated decision making including profiling

The GDPR applies to all automated decision making and profiling processing, and the Care Inspectorate will be aware of this in its digital work.

DATA SECURITY

The Care Inspectorate will take appropriate technical and organisational security measures to safeguard personal information. This will include ensuring appropriate 'safe harbour' arrangements are made should personal data need to be transferred outside of the European Economic Area.

We have established an information security policy and related procedures for both manual records and electronic information, subject to appropriate risk assessment, to ensure that appropriate controls are in place to keep personal data secure at all times, both when it is stored and when it is being shared with or transferred internally or to external parties.

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.

Data Protection Breaches and Complaints

We have robust and documented information incident procedures and controls for identifying, investigating, reviewing and reporting any compliance breaches or near misses.

SHARING PERSONAL DATA

Data processors

Where the Care Inspectorate uses a contractor to process personal data on its behalf, known as a data processor, we must be satisfied that the contractor is taking adequate steps to allow us to meet our obligations under the Regulation.

Contracts between the Care Inspectorate and the data processor must ensure that all necessary security procedures and other appropriate measures are specified in the contract, and that the contract must be monitored to ensure that they are being adhered to.

Sharing Personal Data with other organisations

The Care Inspectorate needs to share personal information with other organisations when fulfilling our statutory functions and obligations or for regulatory reasons when it is lawful and proportionate to do so.

We work closely with other organisations in the health, social care, and social work sectors. We will share information with these organisations for example where we are carrying out joint inspections with partner agencies, investigating complaints or taking enforcement action. The sharing of personal data between the Care Inspectorate and third parties is subject to formal memoranda of understanding and information sharing protocols and agreements. These set out overarching common rules adopted by the Care Inspectorate and its partners with whom it wishes to share data to ensure that this information is properly protected and appropriately, fairly and lawfully handled and disposed of.

A central register of all information sharing protocols and agreements will be maintained by the Information Governance Team to ensure that transfer and sharing arrangements meet the requirements of the General Data Protection Regulation.

All new information sharing protocols and agreements must be reviewed by the Data Protection Officer and approved by the Senior Information Risk Officer before use.

Use of personal data for research, statistical or historical purposes

The Care Inspectorate will inform individuals of their responsibilities when using personal data for research, statistical or historical purposes and will ask them to confirm that they will abide by these terms of access and use.

Disclosure of personal data relating to crime and other unlawful activities

Provisions in the UK Data Protection Act 2018 allow the Care Inspectorate to consider disclosing personal data for the prevention, detection, investigation or prosecution of crime or other unlawful activities.

Each request will be considered on a case by case basis and the information will only be disclosed when it is considered necessary and proportionate to do so. Our overriding consideration will be the protection of people from harm, abuse or neglect.

Unauthorised Disclosure

Employees and others covered by this policy must never disclose personal data obtained in the course of their work with the Care Inspectorate, or access personal data without appropriate permissions. It is a criminal offence to knowingly obtain or disclose personal data without the consent of the data controller - the Care Inspectorate.

PRIVACY BY DEFAULT AND DESIGN

The Care Inspectorate is committed to taking a pro-active approach to privacy and data protection. Core privacy considerations must be integrated into existing project management and risk management methodologies and policies. Data protection impact assessments are used to identify and reduce the privacy risks of any planned changes within the organisation.

We will assess new and existing data processing activities and supporting information systems to ensure that the minimum amount of personal data necessary to achieve the processing purpose is collected and retained for the minimum period necessary.

ACCOUNTABILITY AND COMPLIANCE

The Care Inspectorate will maintain records of our processing activities and compliance action to demonstrating compliance with the GDPR and related privacy legislation.

An inventory of personal data held will be maintained as part of the Information Asset Register. The register will indicate information assets containing personal data and will be used to evaluate and assure compliance with the Care Inspectorate's information governance policy and procedures, including Data Protection, recording and highlighting risk as appropriate.

Designated information asset owners will be accountable for the processing of personal data contained in the information assets for which they are responsible.

Data Protection Officer

As a public authority, the Care Inspectorate has appointed a Data Protection Officer (DPO) as mandated under the Regulation.

The DPO is the named contact for all Data Protection issues and will be able report directly to the Executive Group through the Senior Information Risk Officer.

Engagement with supervisory authority

The Care Inspectorate will engage with the Office of the Information Commissioner directly in policy and process discussions touching on high risk privacy, data sharing and other data protection issues.

Training

The Care Inspectorate will provide eLearning and classroom-based training to ensure that every member of staff understands their data protection responsibilities when using personal data and has the skills to fulfil these.

ROLES AND RESPONSIBILITIES

Executive Group

The Executive Group has overall responsibility for ensuring that all collection and processing within the Care Inspectorate complies with the Regulation and its principles. Responsibility also extends to personal data that is processed by third parties within their respective areas of responsibility. The Executive Group will:

- provide the necessary ownership and advocacy required to support, co-ordinate, promote, monitor and assure compliance with the General Data Protection Regulation.
- review policy and procedures relating to data protection, as appropriate, and ensure that these are reviewed in line with agreed review dates and

any changes to legislation

- review all data breach reports and, where appropriate, make a recommendation to the Care Inspectorate Board through the Chief Executive.

Senior Information Risk Owner

The Executive Director of Strategy and Improvement is the Care Inspectorate's Senior Information Risk Owner (SIRO). The SIRO has delegated authority through the Executive Group with specific responsibility for information risk and mitigation, ensuring that information threats and breaches are identified, assessed and effectively managed.

Data Protection Officer

The Care Inspectorate Data Protection Officer (DPO), who is the named contact for all Data Protection issues and key contact with the supervisory authority, is the Information Governance Lead.

The responsibilities of the DPO are, but not limited to:

- ensuring that the Care Inspectorate Data Protection Policy and related procedures, controls, guidance and templates are kept up to date
- identifying and publicising responsibilities for Data Protection within the Care Inspectorate
- supporting all members of staff, and others covered by this policy, to comply with their obligations under the Regulation
- issuing guidance and training
- monitoring and reporting on the proper functioning of data protection systems.
- acting as the first point of contact for all data protection issues affecting the Care Inspectorate;
- providing guidance and advice on specific data protection issues and compliance requirements

Information Governance Team

The Information Governance Team will support the DPO in maintaining compliance with the General Data Protection Regulation, through implementation of this policy and related procedures, standards and controls.

Information Asset Owners and Line Managers

Information Asset Owners and Line Managers have to day-to-day responsibility for ensuring compliance with the Regulation. Within their respective areas of responsibility, they must:

To fulfil this responsibility they must:

- Ensure that this policy and any associated procedures governing the use of personal information (corporate and local) are in place, understood and followed by all staff within their business areas.
- Ensure that staff receive the data protection training provided
- Inform the Data Protection Officer of the types of personal data held and any changes or new holdings.
- Consult the Data Protection Officer when there is a proposed change in the collection, use and security of personal information, or when new projects are being considered;
- Consult the Data Protection Officer before signing up to, or revising, and information sharing protocol or agreement;
- Report any suspected breaches of confidentiality or information loss following the information security incident procedure
- Identify any existing or emerging information risks relating to personal information and report to the Data Protection Officer and, if required, record on corporate and operational risk registers;
- Ensure that appropriate technical and organisational measures are taken to prevent unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, such data

Staff

Compliance with this Policy is the responsibility of all Care Inspectorate employees and everyone who has access to Care Inspectorate records.

Breaches of this policy and therefore the Regulation, whether deliberate or through negligence, may lead to disciplinary action, in line with Care Inspectorate disciplinary procedures. In serious cases, a breach of the Regulation could also lead to criminal prosecution.

Colleagues must familiarise themselves with and follow this policy as well as the supporting codes of practice, ensure that procedures for the collection and use of personal data is complied with in their area, and familiarise themselves with the implications of data protection in their job.

Legislative Framework

Compliance with this policy will facilitate compliance with the following acts, regulations and standards.

- General Data Protection Regulation
- UK Data Protection Act 2018
- Human Rights Act 1998
- Freedom of Information (Scotland) Act 2002
- Environmental Information Regulations (Scotland) 2004
- Privacy and Electronic Communications Regulations 2003
- Surveillance Camera Code of Practice
- Payment Card Industry (PCI) Data Security Standard 3.1
- Statistics and Registration Service Act 2007
- Equality Act 2010
- Public Records (Scotland) Act 2011
- The Care Inspectorate aims to operate in accordance with HMG Security Policy Framework, HMG Information Assurance (IA) standards and their associated Good Practice Guides / Supplements / IA Notices.
- The Care Inspectorate aims to operate in accordance with the following best practice standards for security and recordkeeping:
    - BS ISO 27001: 2005 - Information Technology - Security Techniques
    - BS EN 15713: 2009 – Secure Destruction of Confidential Material
    - BS ISO 15489-1:2016 - Information and documentation. Records management. Concepts and principles

MONITORING AND REVIEW

This policy will be reviewed every two years or more frequently if required by significant changes in legislation, regulation or business practice. It will be reviewed by the Information Governance Team and presented to the Care Inspectorate Executive Group for approval.