Data Protection & GDPR Policy

Lead/owner	Board of Trustees
Date of Approval	14/03/2024
Author/Reviewer	CEO
Next Rieview date	14/03/2027
Related policies	Confidentiality, Social Media, Telephone Usage, Email and Internet, Risk Management
Level of Approval	Board of Trustees

Policy Statement:

This policy sets out how Compassionate Inverclyde complies with the Data Protection Act 2018 (DPA). This policy aims to fulfil the requirement for fair and lawful processing of personal information in the records which Compassionate Inverclyde creates and receives in the course of our activities.

This policy covers:

• the requirements that must be met for the processing of personal information as set out in the DPA and supplemented and aligned with the General Data Protection regulation (UK GDPR)
• staff responsibilities in relation to data protection
• provision for regular review of the data protection policy and its implementation.

Legal background

The Data Protection Act 2018 establishes a framework of rights and duties which are designed to safeguard personal information. This framework balances the legitimate needs of organisations to collect and use personal information for business and other purposes against the right of individuals to respect for the privacy of their personal details. The DPA imposes obligations on the use of all personal information held by Compassionate Inverclyde and has implications for every part of the organisation. Compassionate Inverclyde is a Data Controller, as defined in Section 1 of the DPA, and is obliged to ensure that all of the DPA requirements are implemented. The DPA applies to all permanent and temporary staff, contractors, volunteers and board members. Compassionate Inverclyde needs to collect and keep certain information about its employees, volunteers, supporters and patients to allow us to conduct our business operations. In order to comply with the law, Compassionate

Inverclyde must ensure that personal information is collected and used fairly, stored safely and not disclosed to any person unlawfully. To do this Compassionate Inverclyde must comply with the eight Data Protection Principles (see below), which are set out in the DPA. Compassionate Inverclyde regards the lawful and correct treatment of personal information as very important to successful business operations, and to maintaining stakeholder confidence.

Relevant legislation and regulations

This policy complies with the following acts, regulations and best practice standards:

• Data Protection Act 2018
• The General Data Protection Regulation 2016 (EU) 2016/679
• Information Commissioner's Office, (2018). Guide to The General Data Protection Regulation (GDPR). Online – https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/
• Human Rights Act 1998
• International Standard on Records Management, ISO 15489
• Society of Archivists and Records Management Society Code of Practice for Archivists and Records Managers
• Scottish Ministers' section 61 Code of Practice on Records Management by Scottish Public Authorities under the Freedom of Information (Scotland) Act 2002

Information subject to the Data Protection Act
DPA relates to the processing of personal data. Personal data is information that both identifies and relates to a living individual and includes any expression of opinion about the individual. The DPA applies to all personal information held electronically and in most manual formats.

The DPA categorises certain types of personal information as sensitive personal information, such as information concerning racial or ethnic origin, religious beliefs, physical or mental health, sexual orientation and criminal records.

Principles:

The DPA sets out eight principles which underpin the handling of personal information. In order to achieve compliance with the DPA, Compassionate Inverclyde must ensure that personal information is:
• processed fairly and lawfully and is not processed unless certain conditions are met
• obtained for specified and lawful purposes and not further processed in a manner incompatible with that purpose
• adequate, relevant and not excessive
• accurate and where necessary up to date
• kept for no longer than necessary
• processed in accordance with the data subjects' rights
• protected by appropriate technical and organisational security measures
• not transferred overseas without adequate protection.

Right of access to personal information

An individual's right to request their own personal information, known as a subject access request (SAR)[1], is set out under section 7 of the DPA. An individual may need to supply proof of their identity before Compassionate Inverclyde can respond to a subject access request. There are certain circumstances when personal information may not be provided if it falls within an 'exemption' in the DPA, other exemptions are set out in Schedule 2 and 3 of the DPA 2018[2]. In any event, Compassionate Inverclyde has to reply to a subject access request within one month of the receipt of the request. However, in circumstances where requests are particularly complex or numerous, Compassionate Inverclyde may be able to extend the time limit to two or three months in total. Where this occurs the data subject will be contacted within one month of their request being received and informed why the deadline is being extended.

Under this right of access, a requester is entitled to be given:
- a copy of the information in permanent form
- an explanation of any technical or complicated terms
- any information about the source of your information, and
- the purposes for processing the information and anyone who the information might be shared with, for example another regulator.

Procedure:

Data protection processes
In order to fulfil its obligations under the DPA, Compassionate Inverclyde has business processes and systems, which:
- Observe fully conditions regarding the fair collection and use of personal information and specify the purposes for which the information is used
- Collect and process appropriate personal information only to the extent that it is needed to fulfil operational needs or to comply with any legal requirement
- Ensure the quality of the personal information which we use and only retain records for as long as we need them
- Ensure that people about whom we hold information can exercise their rights fully under the DPA
- Take appropriate technical and organisational security measures to safeguard personal information
- Ensure that personal information is not transferred abroad without suitable safeguards

[1] When can we refuse to comply with a rehttps://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/when-can-we-refuse-to-comply-with-a-request/quest? | ICO

2

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/#exemptions

This is achieved by:

- The appointment of a Data Protection Officer with specific responsibility for data protection in Compassionate Inverclyde
- The creation of operational guidance for Compassionate Inverclyde staff on handling personal information
- Training for all Compassionate Inverclyde staff in data protection and good practice
- Retention schedules for all Compassionate Inverclyde records to ensure information is only retained for as long as it is required **(see Appendix 1 –retention schedule)**
- The quick and efficient handling of subject access requests.
- Notification with the Information Commissioner of all uses for of personal information within Compassionate Inverclyde
- Adherence to information security procedures for both manual and electronic records
- A regular review and audit of the way in which personal information is collected, stored and used by Compassionate Inverclyde.

Data Processors

Where Compassionate Inverclyde uses a contractor to process personal information on its behalf, the contractor must sign a data processing agreement which ensures that they are taking adequate steps to comply with Principle 7 (and all other DPA requirements) on Compassionate Inverclyde's behalf. Compassionate Inverclyde retains legal responsibility for the actions of processors, and so those managing contracts must ensure that all security procedures necessary are specified in the contract, and it is subsequently monitored to ensure that they are in place.

Staff and Volunteer Responsibilities

All staff and volunteers are required to be aware of the provisions of the DPA and its impact on the work Compassionate Inverclyde undertakes.
Compassionate Inverclyde will:

- Ensure that there is always one person with overall responsibility for data protection. Currently this person is the Data Protection Officer
- Ensure that Compassionate Inverclyde's Data Protection Notification is kept up to date, taking into account and changes in processing of personal data
- Support all members of staff to comply with their obligations under the DPA
- Issue guidance and provide training for Compassionate Inverclyde staff who handle personal data
- Handle requests for personal information quickly and in accordance with the DPA
- Review and update DPA procedures as necessary and in line with changes to UK and EU legislation and case law

All employees, volunteers and trustees will, through appropriate training and

management:

• Familiarise themselves with, and follow all Compassionate Inverclyde guidance, codes of practice and procedures about the collection and use of personal information
• Ensure that procedures for the collection and use of personal information are complied with in their area
• Familiarise themselves with the implications of data protection in their job
• Keep personal information secure
• Collect and process appropriate information, and only in accordance with the purposes for which it is to be used by Compassionate Inverclyde to meet its service needs or legal requirements
• Personal information is not disclosed deliberately or accidentally either orally or in writing to any unauthorised third party
• Promptly forward all initial requests for personal information (known as subject access requests SAR's) to the Data Protection Officer
• Ensure the information is destroyed (in accordance with the provisions of the Act) when it is no longer required
• Not send any personal information outside of the United Kingdom without the authority of the Caldicott Guardian[3]

.

It is a criminal offence to deliberately or recklessly disclose personal information without the authority of the data controller (Compassionate Inverclyde). Managers must ensure that all staff familiarise themselves with the content of this policy.

Any deliberate or reckless disclosure of information by a member of staff or volunteer will be considered as a disciplinary issue.

Board of Trustees

1. The Board of Trustees regard the lawful and correct treatment of personal information as of vital importance to successful business operations, and to maintaining stakeholder confidence.
2. The Board of Trustees has overall responsibility for the Data Protection Policy.
3. The CEO also acts as the Data Protection Officer.
4. The CEO also acts as the Caldicott Guardian
5. All Trustees are responsible for making sure the policy and procedures for handling personal information are followed.
6. The Board of Trustees will make provision for a regular review of Compassionate Inverclyde's Data Protection Policy.

Monitoring and Review:

This policy will be reviewed every three years and it will be ratified through the Board of Trustees.

References:

1. *Data Protection Act 2018*
2. *The General Data Protection Regulation 2016 (EU) 2016/679*

---

[3] The Caldicott Guardian holds a senior role in an organisation which processes personal data in a health and social care setting. Their role is to ensure that personal information about those who use the organisation's services is used legally, ethically and appropriately and that confidentiality is maintained. The Caldicott Guardian provides leadership and informs guidance on complex matters involving confidentiality and information sharing. They are acting as "the conscience of the organisation" and impartiality and independence is central to the advice they impact.

3. *Information Commissioner's Office, (2018). Guide to The General Data Protection Regulation (GDPR). Online –* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/
4. *Human Rights Act 1998*
5. *International Standard on Records Management, ISO 15489*
6. *Society of Archivists and Records Management Society Code of Practice for Archivists and Records Managers*
7. *Scottish Ministers' section 61 Code of Practice on Records Management by Scottish Public Authorities under the Freedom of Information (Scotland) Act 2002*

Document version control

Version number	Change or update	Author or owner	Date
1.0	First version	CEO	14/03/2024