Community Justice Scotland
Data Protection Policy

Date first approved: April 2017
Date of second review: April 2019
Date of third review: August 2022
Date of next review: August 2023

Contents

1. Introduction

Community Justice Scotland and its employees are bound by a legal duty of confidentiality to all data subjects which can only be set aside to meet an overriding public interest, legal obligation, or similar duty.

The General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018 impose obligations on the use of all personal data held by Community Justice Scotland, whether it relates to data subjects and/or their families, employees, complainants, contractors or any other individual who comes into contact with the organisation, defined as data subjects.

In 2011 the ICO published its first Data Sharing Code; in the intervening period the type and amount of data collected by organisations has changed enormously, as has the technology used to store and share it, and even the purposes for which it is used. It is imperative that we keep up to date with these developments through this new code.

In May 2022 the ICO published a new **Data Sharing Code** to give individuals, businesses and organisations the confidence to share data in a fair, safe and transparent way in this changing landscape. This code guides practitioners through the practical steps they need to take to share data while protecting people's privacy.

This GDPR policy sets out how Community Justice Scotland meets its legal obligations and requirements under data protection law. It will be reviewed annually, or as appropriate to take into account changes to legislation that may occur. Any breach of this policy may result in Community Justice Scotland being liable for the consequences of the breach.

2. Roles and Responsibilities

The Chief Executive, as Accountable Officer (AO), has overall responsibility for data protection within Community Justice Scotland. The Director of Operations is designated as Community Justice Scotland's Senior Information Risk Owner (SIRO). The implementation of, and compliance with, this policy is delegated to the Data Protection Officer (DPO). DPO for Community Justice Scotland is the Business Manager.

All data protection and information security related incidents should be reported to the DPO via Cyber Defence and Integrated Security and properly investigated according to the Community Justice Scotland's Security Breach Policy. In the main, correspondence with the Information Commissioner's Office (ICO) on data protection matters will be dealt with by the DPO.

3. The Data Protection Principles

Article 5 of the General Data Protection Regulation outlines the six data protection principles (detailed over) which must be adhered to when processing personal data:

Principle 1 - Process lawfully, fairly and in a transparent manner in relation to individuals

Key considerations

To process personal data at least one of the conditions at Article 6 must be met, and in the case of special category data, at least one of the conditions in Article 9 must be met.

Privacy Notices

When personal information is collected about individuals, they should be told exactly how that information is to be used. This is called a “privacy notice”. This should tell them why Community Justice Scotland needs to process the information.

If individuals know at the outset what their information will be used for, they will be able to make an informed decision about whether or not to enter into the relationship.

Disclosure of personal information

Information about identifiable individuals should only be disclosed on a need to know basis. Disclosures of information may occur because of a legal requirement eg with a Court Order. Specific legislation covers some disclosure (eg for tax and pension purposes).

The validity of all requests for disclosure of personal data without consent from the individual must be checked. The identity of those requesting data and their legal right to request or demand information must be validated. The reasons for disclosures made without consent must be documented.

Police officers or others requesting information for the purposes of a criminal investigation, including for benefit, tax or immigration offences, should be asked to put their request in writing, either by using a standard data protection request form, or by letter / email. This requirement can be set aside where the request is made in an emergency (i.e. a person is in immediate and imminent risk of serious harm).

The request should include:

- What information is needed
- Why it is needed
- How the investigation will be prejudiced without it

Principle 2 – 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

Incompatible re-use of information

Personal data must not be re-used for any purpose that is incompatible with the original purpose it was collected.

Principle 3 - Adequate, relevant and limited to what is necessary in relation for which they are processed

Managers should ensure that any data collected from individuals is complete but not excessive, and the level of data retained on Community Justice Scotland systems should be appropriate for current, existing purposes.

Principle 4 - 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;

Managers must ensure that personal data held on any media is accurate and kept up to date.

Staff information should also be checked for accuracy on a yearly basis – either by line managers or by HR.

Principle 5 - ***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***

Personal data must not be retained indefinitely, and managers must ensure that they are aware of, and compliant with Information Management policy and principles.

Principle 6 - 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

Personal data must be protected from unauthorised access at all times, during collection, storage and transmission. This includes both IT security and physical security.

Security

All information relating to identifiable individuals must be kept secure at all times. Managers must take steps to ensure that office environments and working practices take account of the security necessary to prevent the loss, theft, damage or unauthorised access to personal information. Information Asset Owners (IAOs) are responsible for ensuring that all systems storing personal data, or other assets or repositories of information are appropriately risk-assessed and protected from identifiable threats.

This overarching requirement of accountability requires CJS to maintain adequate records of our data processing activities and keep evidence of how we comply with the data protection principles.

4. Reporting incidents

All data protection and information security related incidents should be reported in writing to the DPO and investigated. In the main, correspondence with the Information Commissioner's Office (ICO) on data protection matters will be dealt with by the DPO, who reports to the Director of Operations.

5. Staff Awareness and Training

Training

All staff must be trained before they can handle personal information in any form in the course of their job.

Community Justice Scotland has adopted the SG mandatory training programme which includes maintaining awareness of data protection and information handling for all staff. This is carried out by annual completion of e-learning as follows:

- Data Protection eLearning package;
- Responsible for Information eLearning package.

6. Disciplinary issues

Employees should be aware that it is a criminal offence to deliberately or recklessly disclose personal data without the authority of Community Justice Scotland (the data controller).

A deliberate or reckless breach of data protection law can result in a member of staff facing disciplinary action. Managers must ensure that all staff familiarise themselves with the content of this policy.

All personal data recorded in any format must be handled securely and appropriately in line with the data protection law, and staff must not disclose information for any purpose outside their normal work role. Any deliberate or reckless disclosure of information by a member of staff will be considered as a disciplinary issue.

Karyn McCluskey
Chief Executive, Community Justice Scotland
August 2022