
2021/25

# Data Protection & Information Sharing Policy

# CONTENTS

# 1. PURPOSE

This policy sets out how the organisation acquires, records, stores, discloses, and destroys data in line with the Data Protection Act (DPA) and the UK's implementation of the General Data Protection Regulation (GDPR).

# 2. AUDIENCE

This policy is intended for:

- all members of the workforce (including trustees, staff, volunteers, and contractors)
- service users

# 3. RELATED DOCUMENTS

This policy should be read alongside:

- Data Protection Act 2018
- General Data Protection Regulation 2016/679
- The ICO guide to GDPR

# 4. DEFINITIONS

For the purposes of this policy, the following definitions apply:

## 4.1 Service Users

The individuals who receive support from the organisation. This includes survivors and their family or friends. The terms 'person', 'client' and 'victim' are also included in this definition.

## 4.2 Data Subjects

The individuals who the organisation collects information on. This includes the workforce and service users, alongside contractors and suppliers of various kinds.

## 4.3 Personal and Sensitive Information

Data which can identify an individual and sensitive information includes the person's race or ethnicity, political opinions, religious beliefs, trade union membership, physical or mental health, sexual life, the commission or alleged commission of any offences and details of criminal proceedings.

## 4.4 The Organisation

For the purposes of this policy 'the organisation' refers to Clean Slate

## 5. BACKGROUND

The organisation collects and uses information about the people with whom we deal. We also acquire information about others during those dealings. The information can be factual, such as name and address, or expressions of opinion about or intentions towards individuals and can be in any form or format (WORD documents, databases and spreadsheets, emails, index cards, paper files etc.).

All the workforce and service users have an individual responsibility to uphold the legal requirements of the DPA and GDPR. Breaches may lead to disciplinary action being taken and, possibly, to prosecution of the individual concerned.

## 6. DATA PROTECTION PRINCIPLES

Everyone responsible for using personal data has to follow strict rules called 'data protection principles. These principles are:

- Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless certain conditions are met.
- Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any matter incompatible with that purpose or those purposes.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- Personal data shall be processed in accordance with the rights of data subjects under this Act.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data shall not be transferred to a country or territory outside the European Economic Area (EEA) unless that country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

## 7. SENSITIVE DATA

The organisation will collect and process sensitive personal data only when required to do so by law or when needed in connection with operational requirements.

There is stronger legal protection for more sensitive information, such as:

- race
- ethnic background
- political opinions
- religious beliefs
- trade union membership
- genetics
- biometrics (where used for identification)
- health
- sex life or orientation

There are separate safeguards for personal data relating to criminal convictions and offences.

# 8. RECRUITMENT

Job descriptions, job contracts and volunteer agreements make it clear that they are bound by the provisions of the Data Protection Policy and that acceptance of the contract/completion of the training signifies consent to processing data.

- **Abuse of Privilege**

It is strictly forbidden for staff to knowingly browse, search for or look at any personal or confidential information about themselves without a legitimate purpose, unless it is through established self-service mechanisms where such access is permitted (e.g. viewing your record). Under no circumstances should staff attempt to access records relating to family members, friends or other known persons without a legitimate purpose and it being undertaken by an independent third party. Action of this kind will be viewed as a breach of confidentiality and may be an offence under the Data Protection Act 2018. When dealing with person-identifiable or confidential information of any nature, staff must be aware of their personal responsibility, contractual obligations and undertake to abide by the policies and procedures of NHSCFA. Confidentiality audits provide mechanisms that allow an organisation that processes person-identifiable or confidential information to test the processes it has in place to highlight actual or potential confidentiality breaches of their systems and the procedures to evaluate the effectiveness of their system controls. This function may be performed by external auditors or internally by the Governance and Assurance (G&A) team through a programme of agreed audits.

- **Confidentiality is an obligation for all volunteers and staff.**

Volunteers and staff should note that they are bound by Confidentiality:
Volunteer Code of Practice. There is generally a confidentiality clause in contracts of employment, and it is mandatory to participate in induction, e-learning and awareness raising sessions carried out to inform and update staff on confidentiality issues.
Any deliberate breach of confidentiality, inappropriate use of client data, staff records or business sensitive/confidential information, or abuse of computer systems is a disciplinary offence, which could result in dismissal and must be reported to an appropriate line manager. Where a duty of confidence is broken or breached, civil legal action may be taken against those responsible in order to secure financial recompense.

Section 170 (1) of the Data Protection Act 2018 - Unlawful obtaining etc. of personal data, states it is an offence for a person knowingly or recklessly:
to obtain or disclose personal data without the consent of the controller to procure the disclosure of personal data to another person without the consent of the controller, or after obtaining personal data, to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained. It is important to note that there may be situations where both the organisation and the individual concerned can be held liable.

## 9. SECURITY

All data held by the organisation will be kept securely, whether kept by an individual or in the organisation's offices. Any recorded information on service users or the workforce shall be:

- kept in locked cabinets; *or*
- protected by the use of passwords if kept electronically.

Access to information on a computer system is controlled by a password and only those needing access are given the password. Staff should be careful about the information that is displayed on a computer screen and make efforts to ensure that no unauthorised person can view the data when it is on display.

## 10. RETENTION OF DATA

The organisation will only keep records containing personal sensitive data if they are relevant to the organisations aims and objectives. The retention time will vary depending on the type of data.

## 11. DISPOSAL OF DATA

When personal data is no longer to be retained it will be disposed of in such a way that the rights and privacy of the individual concerned are protected, e.g. disposal by shredding, burning, secure electronic deletion.

## 12. PUBLICLY AVAILABLE INFORMATION

The provisions of the DPA do not extend to information already in the public domain. Such information includes:

- Names of all members of the Management Committee.
- Name, initial(s), and job title as listed in various publications issued by the organisation, e.g. training programmes, service directories, Awards and honors' relating to work done for the organisation.
- Information about the organisation which is publicly available, including names of staff members.

## 13. RIGHTS OF ACCESS TO DATA

Under the DPA you have the right to find out what information an organisation has about you. These include the right to:

- be informed about how your data is being used

- access personal data
- have incorrect data updated
- have data erased
- stop or restrict the processing of your data
- data portability (allowing you to get and reuse your data for different services)
- object to how your data is processed in certain circumstances
- You also have rights when an organisation is using your personal data for:
- automated decision-making processes (without human involvement)
- profiling, for example to predict your behaviour or interests

In most cases you cannot charge a fee for data subject requests. However, you can charge a 'reasonable fee' for the administrative costs of complying with a request if it is manifestly unfounded or excessive, or if an individual requests further copies of their data. Any such request will be normally be complied with within 40 days of receipt of the written request and, where appropriate, the fee.

The Freedom of Information Act (FOI) provides individuals and organisations with a right of access to information held by public services. Charities that deliver public services are however exempt from the Act and therefore do not have to respond to any request for information under the FOI.

## 14. INFORMATION SHARING

The data subject shall be advised what information may be shared and the reasons why.

The data subject should be asked to consent to the sharing of their information. If the data subject is a child, the professional needs to be satisfied that the child understands what it means to consent or refuse the sharing of information. Consent may be given by another person on behalf of the data subject if they are not capable of exercising their rights independently.

Information may be shared without the consent of the data subject if:

- the sharing of information is required by law through a statutory duty or by a court order; *or*
- it is in the public interest to do so. For example, if seeking consent would place the data subject at risk of significant harm, prejudice the prevention, detection or prosecution of a serious crime or lead to an unjustifiable delay in making enquiries about allegations of significant harm to a child.

The facts of the individual case should be considered when deciding whether to share information without consent. The safeguarding of the individuals involved should be the main consideration. Guidance on making this decision can be found in Appendix A and the ICO website.

The discussions and consent or refusal to share information shall be recorded in writing. Information must be accurate and necessary for the purpose for which it is being shared and shared only with those who need to see it.

# 15. APPENDIX A – DECISION CHECKLIST

The below considerations may assist with the decision about whether to share information. The safeguarding of the data subject should be the primary consideration in all decision making about information sharing.

The below checklist is sourced from the Information Commissioner's Office, Data Sharing Checklists, licensed under the Open Government License.

## 1. Is the sharing justified?

Key points to consider:

- Do you think you should share the information?
- Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?
- Do you have concerns that an individual is at risk of serious harm?
- Do you need to consider an exemption in the DPA to share?

## 2. Do you have the power to share?

Key points to consider:

- The type of organisation you work for.
- Any relevant functions or powers of your organisation.
- The nature of the information you have been asked to share (for example was it given in confidence?).
- Any legal obligation to share information (for example a statutory requirement or a court order).

## 3. If you decide to share

Key points to consider:

- What information do you need to share?
  - Only share what is necessary.
  - Distinguish fact from opinion.
- How should the information be shared?
  - Information must be shared securely.
  - Ensure you are giving information to the right person.
- Consider whether it is appropriate/safe to inform the individual that you have shared their information.

## 4. Record your decision

Record your data sharing decision and your reasoning – whether or not you shared the information. If you share information you should record:

- What information was shared and for what purpose.
- Who it was shared with.
- When it was shared.
- Your justification for sharing.
- Whether the information was shared with or without consent.

# 1. VERSION HISTORY

It is recommended that this document is reviewed at minimum every 3 years. However, legal updates may need to be incorporated more frequently.

| Version | Date | Approved by |
|---|---|---|
| 1.0 | 02/02/2021 | Nadia Brown - Project Manager |
| 2.0 | 01/04/2023 | Nadia Brown - CEO |