Data Protection Policy

May 2018

Version:	1.0 Final approval
Author:	IG Team
Approved by:	Senior Information Risk Owner (SIRO) Board
Date approved:	18th April 2018
Review date:	25th May 2019
Target audience:	All Staff / Elected Members / Citizens

Contents

1. Summary

This policy sets out how the trust will comply with data protection legislation and protect the personal information of everyone who receives services from, or provides services to, the trust. It informs customers of their rights, and suppliers of their responsibilities. It shows how we comply with the General Data Protection Regulation (GDPR), the Data Protection Act 2018, other regulations and good practice standards.

2. Scope

This policy applies to employees, contractors, agency workers and staff.
It covers personal data we collect and use on paper and electronically. It covers our corporate databases, computer network and archive of paper records. It covers video and photographs, voice recordings and mobile devices such as laptops, mobile phones and memory sticks.

3. Accountability

The Trust is a data controller which means that it decides why and how personal data is processed. The Trust is also a joint data controller with Doncaster Council. The Trust is accountable for its handling of personal information.

Our *Chief Executive* is the person accountable for providing the policies for employees to follow under the law, so that we can carry out decisions of the Trust Board and council in response to our statutory functions. The Data Protection Policy is part of our corporate governance framework, which contains important policies and procedures maintained and published by the Trust, that are key to good governance and effective decision making.

The *Senior Information Risk Officer* (SIRO) is the Director of Children's Social Care who is accountable for protecting the Trust's information assets.

The *Caldicott Guardian* is the Director of Children's Social Care. The Caldicott Guardian is responsible for protecting the confidentiality of people's health and social care information and making sure it is used properly.

The *SIRO Board* is made up of various senior members of staff and gives strategic guidance to the SIRO and Caldicott Guardian for the management of the Trust's information assets. The SIRO Board gives direction to Information Asset Owners who are Heads of Service.

The *Data Protection Officer* is a position required in law to ensure the Trust complies with data protection legislation and acts as a single point of contact for individuals who want to find out about their data. (See also section 23)

Each *employee and supplier* is bound by a contractual duty of confidentiality.

The Trust is registered with the *Information Commissioner*, who is the independent regulator appointed by parliament to check compliance with data protection law.

The Trust maintains a *register of processing activities (information asset register)* of the personal information we are responsible for to ensure it is used according to the data protection principles.

4. Data protection is a fundamental right

The protection of a person's data is a fundamental right. Under the Human Rights Act 1998, everyone has the right to respect for their private and family life, their home and their correspondence. This includes respect for your private and confidential information, particularly when storing and sharing data.

This right can be limited in certain circumstances but any limitation must balance the competing interests of an individual and of the community as a whole.

In particular any limitation must be covered by law and be necessary and proportionate for one or more of the following aims:

- public safety or the country's economic wellbeing
- prevention of disorder or crime
- protecting health or morals
- protecting other people's rights and freedoms
- national security.

The right to privacy must often be balanced against the right to free expression. Public figures don't necessarily enjoy the same privacy as others. For example, sometimes the public interest might justify publishing information about senior officers that would otherwise interfere with their right to privacy.

5. Personal data

In this policy we use the terms "personal data" and "special categories of personal data" which are used in data protection legislation.

In this policy personal data means any information relating to an identifiable living person. This means they can be identified from information such as a name, an address, an identification number (e.g. your National Insurance number, NHS number or case reference number), location data, etc.

"Special categories of personal data" is personal sensitive data. This is data regarding an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data and biometric data (fingerprints, eye scans etc.) for the purpose of uniquely identifying a person, data concerning health or data concerning a person's sex life or sexual orientation.

There are extra safeguards for special categories of personal data to ensure no one is discriminated against when it comes to receiving a service.

We generally refer to a person or individual in this policy, although the term in law is “data subject”.

The frequent reference in this policy to “processing” data means any operation performed on personal data, whether using a computer or manual filing systems. It includes collection, use, and recording, storing, sending and deleting personal data.

6. Data protection principles

The Trust applies data protection principles in its processing of personal data. These principles are set out in the General Data Protection Regulation and have been incorporated into the Data Protection Act 2018. The six principles are that personal data should be:

- Processed lawfully, fairly and in a transparent way
- Collected for a specific purpose
- Adequate, relevant and limited to what’s necessary
- Kept up to date
- Kept for only as long as necessary
- Protected with appropriate security.

7. Lawful basis of processing personal data

There are different lawful reasons for processing personal data and special categories of personal data. The Trust always uses at least one lawful basis for processing personal information and at least one lawful basis for processing special categories of personal data.

The six lawful reasons for processing personal data are:

a) An individual has given consent for the processing of his or her personal data, and it is freely given, specific, informed, and there must be an indication signifying agreement;

b) the Trust has a contract with a person and need to process their personal data to comply with our obligations under the contract; or we haven’t yet got a contract with the person, but they have asked us to do something as a first step (e.g. provide a quote) and we need to process their personal data to do what they ask;

c) The Trust is obliged to process personal data to comply with the law. We will always refer to the specific legal provision or source of advice that explains generally applicable legal obligations;

d) The processing of personal data is necessary to protect someone’s life (“vital interests”);

e) The processing of personal data is necessary under public functions and powers set out in law; or the Trust needs to perform a specific task in the public interest that is set out in law;

f) The processing of personal data is in the llegitimate interests of the Trust, where we use your data in ways that people would reasonably expect and that have a minimal privacy impact. However, public authorities are more limited than private organisations in their ability to rely on this basis for processing personal data;

The lawful bases for processing special categories of data are:

(a) an individual has given explicit consent to the processing of personal data for one or more specified purposes, except where limited by law;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Trust or a person under employment, social security and social protection law or a collective agreement under law;

(c) processing is necessary to protect the vital interests of a person or where the person is physically or legally incapable of giving consent;

(d) processing by non-for-profit bodies for legitimate activities with appropriate safeguards;

(e) processing relates to personal data which have been made public by a person;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest under law;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of law or pursuant to contract with a health professional and subject to the duty of confidentiality;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, subject to the duty of confidentiality;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes;

The Trust must always demonstrate it processes information with safeguards in place to protect the fundamental rights and interests of the individual.

8. Consent

Where the Trust relies on consent or explicit consent as the lawful basis for processing, we will do this to by offering individuals real choice and control.

We will avoid making consent to processing a precondition of a service.

We will be clear and concise.

We keep our requests for consent separate from other terms and conditions.

We will be specific and ‘granular’ so that we get separate consent for separate things.

We will name any third parties (i.e. other groups or organisations) who will rely on the consent.

We will make it easy for people to withdraw consent and tell them how.

We will keep evidence of consent (who, when, how, and what we told people).

We will keep consent under review, and update it if anything changes.

For explicit consent we will ensure the individual provides a very clear and specific statement of consent.

9. Duty of confidentiality

Our staff abide by a common law duty of confidentiality. This means that personal information that has been given to a member of staff or the Trust by an individual should not be used or disclosed further, except as originally understood by that individual, or with their permission.

Our staff are subject to a Code a Conduct relating to confidentiality. Staff have a confidentiality clause in their contracts.

Our caring professions are further subject to the professional codes of conduct of their professions relating to the confidentiality of their relationship with service users and clients.

10. Information about criminal offences

The processing of information about criminal allegations, convictions or offences by the Trust is in accordance with our legal obligations and because we have legal authority in certain areas, such as police referrals. We have a separate policy for the processing of this data.

11. Children

The Trust pays particular protection to the collecting and processing of children's personal data because they may be less aware of the risks involved.

Where we offer an online service, which is not a preventive or counselling service, directly to a child, only children aged 13 or over are able provide their own consent. For children under this age we obtain consent from whoever holds parental responsibility for the child.

12. Automated processing

If the Trust relies on automated decision-making (making a decision solely by automated means without any human involvement) which affects an individual, we inform the individual; introduce simple ways for them to request human intervention or challenge a decision; and carry out regular checks to make sure that our systems are working as intended.

13. How we handle personal information - Privacy notices

The Trust provides privacy notices, which are statements to individuals about the collection and use of their personal data. The information includes our purposes for processing their personal data, retention periods for that personal data, and who it will be shared with.

This information is on the Trust's website, and individuals are referred to it at the time we collect their personal data from them.

Where we obtain personal data from other sources, we provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month.

14. Individual Rights

Individuals whose data is processed by the Trust have a number of rights in law.

(a) The Trust will respond to a request by an individual for access to the information we hold about them. We will respond within one month. We may take longer than one month and up to three months if the request is complicated, and we will inform you of this. There is no charge for this service. We will provide the information in secure electronic format unless you prefer otherwise. We will explain why we process your data, the lawful basis for doing so, who sees it and how long we keep it for.

(b) The Trust will respond within one month to a request from an individual to have inaccurate personal data rectified (corrected), or completed if it is incomplete. Where the Trust can lawfully refuse to rectify the data, we will explain why.

(c) The Trust will respond within one month to a request from an individual to have personal data erased. Where the Trust can lawfully refuse to erase the data, we will explain why.

(d) The Trust will respond within one month to a request from an individual to move, copy or transfer personal data easily from the Trust's computer network to another in a safe and secure way. We will do this in a structured, commonly used and machine readable form and free of charge.

(e) The Trust will consider a request from an individual objecting to the processing of their personal data in relation to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

We shall ensure that individuals know about their right to object when we first tell them about the processing and in our privacy notice.

15. Information sharing

The Trust believes that the duty to share information can be as important as the duty to protect information. This is the seventh Caldicott Principle, which applies to the handling of personal confidential information. Its purpose is to ensure that the direct care of people should not be impeded where professionals from different organisations such as social workers, nurses and community mental health workers need to support an individual.

We have signed Information Sharing Protocols setting out the principles of information sharing with partners, such as the police, health, probation, prisons, Department of Work and Pensions, and the Department of Communities and Local Government.

These protocols are supplemented by Information Sharing Agreements at the point at which data is shared. These set out what data is being shared, how it is transferred and the retention period.

16. Transfers to other countries

Most of our processing occurs in the UK or European Union. This means that there are common standards for the processing of personal data. However, when personal data is transferred to third countries, the Trust assures itself that there is a level of adequacy in the data protection arrangements of that country.

17. Privacy by design

The Trust is committed to a privacy by design or privacy by default approach to building new systems and updating procedures for processing personal data. We use the best technology and human processes we can in order to limit the risks to privacy.

18. Data Protection Impact Assessments

The Trust requires all its services to carry out Data Protection Impact Assessments (DPIAs) when they introduce new technology or changes to the processing of personal data. The assessment identifies the risk to privacy from the customer's perspective and what steps can be taken to reduce this wherever possible whilst providing a service to the customer. We will consult users. We will publish DPIAs on our website. We will treat them as living documents to be revised and updated whenever necessary.

19. Contractors

Where the Trust has a contractual relationship with another organisation or individual, we will ensure we are clear about the contractor's role, responsibilities and accountability in relation to personal information.

20. Information Security

The Trust receives ICT services from the council through a service level agreement. The council ensures there are appropriate measures in place to protect personal data.

The Council has an Information Security policy. The purpose of this policy is to take appropriate technical and organisational measures to protect personal data.

The council obtains independent assurance of its information security and complies with the information security standards of the Public Service Network.

The council has government Cyber Essentials accreditation.

The council meets the standards of PCI-DSS, which is the standard for protecting credit and debit card payments.

The council complies with the Data Security and Protection Toolkit of the Department of Health/NHS for handling personal confidential data.

21. Breaches

The Trust tries hard to prevent information breaches, but when these occur, there is an incident reporting procedure. Breaches are reported to Heads of Service. Where a breach is a serious risk to the rights and freedoms of anyone, it will be reported to the Information Commissioner within 72 hours.

22. Data Protection Officer

The Trust has appointed a Data Protection Officer as required by law. Their role will be to ensure the compliance of the Trust with data protection law.

The Trust Data Protection Officer can be contacted at: DCSTDPO@dcstrust.co.uk Tel 01302 735954.

The council's Data Protection Officer and the Information Governance Team can be contacted at: information.governance@doncaster.gov.uk Tel 01302 736000.

23. How to complain

If you think we have breached data protection, you can complain. The complaint will be investigated by a Head of Service independent of the service which provided the original response. We will respond within one month.

If you are still unhappy, the Data Protection Officer will consider your appeal. Their response will take up to one month.

Finally, individuals can take their complaint to the Information Commissioner's Office for a decision.

24. Service and benefit

Data protection is a big challenge when digital technology can collect and transmit huge volumes of personal data. For our staff, managers and senior officers we are positive about the benefits, and serious about our responsibilities. We are transparent and accountable, and we believe that we can both serve, and protect, the information of our citizens and service users.

25. References

Regulation (EU) 2016/679 (General Data Protection Regulation)

Data Protection Act 2018

Directive (EU) 2016/680 Law Enforcement Directive

The Caldicott Principles www.ukgc.uk

Information Commissioner's Office: www.ico.org.uk

26. List of related policies and procedures

The Data Protection Policy should be read with the following policies:-

Safeguarding Special Category Data Policy
Law Enforcement (Data Protection) Policy
Information Security Policy
Information and Records Management Policy
Rights of Individuals Policy
Data Protection Impact Assessment Procedure
Tier One Information Sharing Protocol
Tier Two Information Sharing Agreement