Chizuk Data Protection Policy.

Reviewed March 2025 Next Review Date March 2026

Chizuk endorses the 7 Caldicott Principles for the protection of personal data; is registered with the ICO and has policies and procedures fully compliant with the Data Protection Act, GDPR, and other relevant legislation.

1. Justify the purpose(s) Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.
2. 2. Don't use personal confidential data unless it is absolutely necessary Personal confidential data should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).
3. 3. Use the minimum necessary personal confidential data Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data transferred or accessible as is necessary for a given function to be carried out.
4. 4. Access to personal confidential data should be on a strict need-to-know basis Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.
5. 5. Everyone with access to personal confidential data should be aware of their responsibilities Action is taken to ensure that those handling personal confidential data – both staff working directly with the client; and staff based in the office – are made fully aware of their responsibilities and obligations to respect client confidentiality.
6. 6. Comply with the law Every use of personal confidential data must be lawful. The Executive Officer of Chizuk is responsible for ensuring that the organisation complies with legal requirements for handling personal confidential data.
7. 7. The duty to share information can be as important as the duty to protect patient confidentiality Health and social care professionals should have the confidence to share information in the best interests of their clients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

The challenges of working within the boundaries of confidentiality should not impede taking appropriate action. Whenever possible, informed consent to the sharing of information should be obtained. However: A Emergency or life-threatening situations may warrant the sharing of relevant information with the relevant emergency services without consent. B The law does not prevent the sharing of sensitive, personal information within organisations. If the information is confidential, but there is a safeguarding concern, sharing it may be justified. C The law does not prevent the sharing of sensitive, personal information between organisations where the public interest served outweighs the public interest served by protecting confidentiality – for example, where a serious crime may be prevented. Whether information is shared with or without the adult at risk's consent, the information sharing process should abide by the principles of the Data Protection Act 2018. In those instances where the person lacks the mental capacity to give informed consent, staff should always bear in mind the requirements of the Mental Capacity Act 2005vii, and whether sharing it will be in the person's best interest.

Definitions and explanations

Data means information which –
(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,
(b) is recorded with the intention that it should be processed by means of such equipment,
(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,
(d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68, or
Paragraphs (a) and (b) make it clear that information that is held on computer, or is intended to be held on computer, is data. So data is also information recorded on paper if you intend to put it on computer. Relevant filingany set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible. system (referred to in paragraph (c) of the definition) is defined in the Act as: Accessible records were included in the definition of “data” because pre-existing access rights to information were not restricted to automatically processed records, or records held in non-automated systems falling within the definition of “relevant filing systems”. So, to preserve all these pre-existing access rights, the definition of “data” covers accessible records even if they do not fall in categories (a), (b), or (c).

Personal data means data which relate to a living individual who can be identified –

(a) from those data, or
(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,
and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.
Sensitive personal data means personal data consisting of information as to -

(a) the racial or ethnic origin of the data subject,
(b) his political opinions,
(c) his religious beliefs or other beliefs of a similar nature,
(d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
(e) his physical or mental health or condition,
(f) his sexual life,
(g) the commission or alleged commission by him of any offence, or
(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.
Processing, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including –

(a) organisation, adaptation or alteration of the information or data,
(b) retrieval, consultation or use of the information or data,
(c) disclosure of the information or data by transmission, dissemination or otherwise making available, or
(d) alignment, combination, blocking, erasure or destruction of the information or data.

The Data Protection Act protects the rights of individuals whom the data is about (data subjects), mainly by placing duties on those who decide how and why such data is processed (data controllers).
The Data Protection Act 2018 should not be a barrier to sharing information. It provides a framework to ensure that personal information about living persons is shared appropriately
Data subject means an individual who is the subject of personal data.
Data controller means … a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

A data controller must be a “person” recognised in law, that is to say:

- individuals;
- organisations; and
- other corporate and unincorporated bodies of persons.

Data controllers will usually be organisations, but can be individuals, for example self-employed consultants. Even if an individual is given responsibility for data protection in an organisation, they will be acting on behalf of the organisation, which will be the data controller.
In relation to data controllers, the term jointly is used where two or more persons (usually organisations) act together to decide the purpose and manner of any data processing. The term in common applies where two or more persons share a pool of personal data that they process independently of each other.
Data controllers must ensure that any processing of personal data for which they are responsible complies with the Act. Failure to do so risks enforcement action, even prosecution, and compensation claims from individuals.

> **Data processor**, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.