Scarborough & Ryedale Carers Resource

# Data protection and subject access guidance

This document is provided by *Scarborough and Ryedale Carers Resource* (now referred to as 'the organisation').

## Contents



**1.0 SCOPE**

1.1 This guidance sets out the approach Scarborough & Ryedale Carers Resource (SRCR) takes in relation to service user data held by the organisation. The term 'service user' includes parents, carers and people of all ages with care needs.

1.2 Data protection law has undergone significant changes in recent times. The EU General Data Protection Regulation 2016/679 (GDPR) comes into force on 25 May 2018 and will have direct effect in all EU Member States from that date onwards, without the need for any national legislation. However, the GDPR will be supplemented by a new Data Protection Act due to be passed through Parliament on or around the date the GDPR comes into force.

1.3 The guidance aims to make sure that the organisation obtains, stores, uses, discloses and disposes of personal data about living individuals in line with legislative requirements, no matter how that information is held.

1.4 The intended outcome of the data protection and subject access policy documents is that the organisation obtains, stores, uses, discloses and disposes of personal data about living individuals in line with legislative requirements, no matter how that information is held.

1.5 This document applies where an individual seeks to obtain a copy of their own personal information (a subject access request) or where a third party has either been asked by the individual to act on their behalf (as a representative) or has been lawfully appointed to act on the individual's behalf (for example through Power of Attorney or Court of Protection Order). They are also relevant where a parent / legal guardian or person with parental responsibility acts on behalf of a child to make a subject access request for that child's personal information.

1.6 This policy will be read in conjunction with the confidentiality and disclosure policy documents. These address situations where a third-party individual or other organisation seeks to obtain disclosure of an individual's personal data held by the organisation, termed 'data sharing' by the Information Commissioner's Office (ICO)

## 2.0 TERMS USED

2.1 **Personal data**

Personal data is anything that identifies a living person either on its own or by reference to other information.

2.2 **Special categories of personal data**

Some personal data is more sensitive than others. It includes for example facts about a person's religion or their medical condition.

2.3 The above categories of data can apply to any individual and may include the following, though the list is not exhaustive:

- carers, family members, people of all ages with care needs
- employees
- volunteers
- trustees
- donors
- supporters
- people from other organisations.

## 3.0 GENERAL DATA PROTECTION REGULATION (GDPR)

3.1 The organisation is required to nominate a Data Protection Officer / Caldicott Guardian (DPO / CG) and deputy to deal with data protection and subject access issues. If you don't know who this is or would like more information, speak to your line manager.

3.2 All data must be collected, processed, maintained, stored, disclosed and disposed of according to the GDPR, as set out below.

3.3 HOLDING personal data / special categories of sensitive data

The organisation is**:**
only allowed to use it for the purpose/s for which it was originally obtained
required to take good care of it to maintain confidentiality
required to use it 'fairly' and 'lawfully'
required to keep records no longer than necessary.

You are committing an offence if you:
gain access to personal data / special categories of personal data you are not authorised to look at
disclose information 'knowingly or recklessly' to people not authorised to see it
sell personal data / special categories of personal data you are not entitled to.

3.4 OBTAINING personal data / special categories of personal data
It must be verified that**:**

- the person providing the data knows it is being collected and how / why it will be used
- if data is from someone other than the person it is about, that person knows who is using their data and how / why it will be used
- necessary consent is obtained to use collected data.

3.5 DISCLOSING (telling anyone else about) personal data / special categories of personal data
It must be verified that**:**

- any disclosure fits with the purpose/s for which the data is held – if not, refer the person requesting the information to the DPO / CG or deputy (see 3.1 above)
- the person requesting the information is authorised to have access to it
- the person the data is about is aware that this kind of disclosure is possible or that there is an over-riding reason (such as a legal obligation) to disclose the information.

3.6 In addition to the above:

- if consent is needed before information can be disclosed, it cannot be disclosed if consent is denied, but the consequences of the decision not to disclose can be explained
- if data is to be transferred outside of the European Economic Area special rules apply.

3.7 If you are asked to disclose personal / sensitive data and are unsure whether you are allowed to do so, or are unsure about any of the above, check it out with your line manager or the DPO / CG first.

**4.0 LEGISLATION**

4.1 The organisation will seek to comply with the GDPR in the way it collects, processes, maintains, stores and disposes of data, ensuring it is:

- processed lawfully, fairly, and in a transparent manner
- collected for specified, explicit and legitimate purposes
- adequate, relevant and limited to what is necessary for the purpose for which the data is processed
- accurate and where necessary kept up-to-date
- not kept for longer than is absolutely necessary for its given purpose
- subject to appropriate security to safeguard against unauthorised or unlawful use, destruction or damage

The organisation is also required to demonstrate how it is complying with its obligations under the GDPR, by ensuring that appropriate systems, controls and procedures are in place.

4.2 The organisation will also seek to comply with the Caldicott Principles, which apply to regulated care and support services and govern the use and management of personal information that allows an individual to be identified. The organisation will:

- be able to justify the purpose of how they use and manage such information
- not use it unless it is necessary
- use the minimum necessary amount of information
- ensure it is accessed on a strict need-to-know basis
- ensure those accessing such information are aware of their responsibilities
- understand and comply with the law
- be aware that the need to share information can be as important as the duty to protect an individual's confidentiality.

4.3 The organisation is required to nominate a Data Protection Officer / Caldicott Guardian (DPO/ CG) and maintain an up-to-date register entry with the ICO in so far as this requirement continues to apply (ceases on 25 May 2018).

The DPO must be selected on the basis of professional qualities and expert knowledge of data protection law, but does not need to be legally qualified. In particular, the DPO must fulfil the tasks set out in Appendix 1 and must:

- be informed of all data protection issues within the organisation in a proper and timely manner
- be provided with the necessary resources to carry out his / her tasks and have access to all personal data operations
- have autonomy to undertake his / her tasks
- report to the highest level of management and not be dismissed or penalised for performing his / her tasks
- be accessible, as data subjects (see definition in A03b – Appendix 1) may contact the DPO with regard to all issues relating to processing and the exercise of their rights

4.4 With regard to data protection and the processing of confidential information, the organisation will also, where applicable, seek to comply with:

- Care Standards Act 2000
- Care Act 2014
- Domiciliary Care Agencies (Wales) Regulations 2004
- Health and Social Care Act (2008) and the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014
- Protection of Freedoms Act 2012
- Human Rights Act 1998
- Mental Capacity Act 2005
- Access to Health Records Act 1990
- Privacy and Electronic Communications Regulations 2003

**5.0 SUBJECT ACCESS RIGHTS OF DATA SUBJECT**

5.1 Where personal information is kept, the individual to whom it applies has the right to access it and (amongst other rights) is entitled to correct any error or omission. This applies to records

kept in the organisation's office/s and those kept in service users' homes. See accompanying procedure (A03b) for details.
Service users are entitled (amongst other rights) to have access to personal data held about them. This is called 'subject access'.

5.2 The DPO / CG will respond to a subject access request within one month of receiving it. There will not normally be a charge for this, unless for example the request were unfounded or excessive.

**6.0 GENERAL RECORD KEEPING**
6.1 It is best to word process records wherever possible. Where hand-written records are unavoidable, they need to be:

- written in black ink
- readable.

6.2 When you record anything, check that what you are writing / word processing is:

- accurate
- factual
- relevant
- not too long
- up to date
- treated confidentially.

6.3 Make sure what you write is understandable and describes the true situation. Don't use shorthand, abbreviations or note form as it may not make sense to the people reading it.

6.4 Think very carefully before you put your personal opinions into writing and don't do so unless you have a good reason. Bear in mind that recorded opinions about another individual form part of that person's personal data and could be disclosed to them if they ask to see their file. You will need to be able to show that your opinions are based on facts and that they are genuinely relevant to the situation.

6.5 Where applicable, records and notes (including care and support plans) need to be signed and dated. If you see any unsigned records or notes, let your line manager know.

6.6 Make sure each record sheet relating to a particular person has their name on it.

6.7 Try to write up records as soon as possible after the event or decision they relate to, when you can clearly remember the facts.

6.8 If you think a piece of recorded information is not accurate, let your line manager know.

**7.0 HOME VISITS**
7.1 If your job includes going into service users' homes (for example to carry out assessments or reviews or to supervise staff), keep a record of the visits you make.

- Record the date and time of your visit, why you visited and any other relevant information, using for example the client report form kept in the home.
- Where possible, do this in the presence of and with the permission of the person concerned.

- Sign / initial your entry and ask the service user or their representative to sign it as well, to verify that what you have written is accurate.
- Ensure any paperwork that needs to stay in the home is put away securely but remains accessible by those who may need to refer to it.

**8.0 CONFIDENTIALITY**

7.1 Treat documents and records containing personal information that would allow an individual to be identified as confidential and take care to keep them secure. This includes anything containing a service user's details (for example time sheets, files or equipment on which information is stored, such as laptops) which, if lost or stolen, could put them at risk of harm.

8.2 If you are working outside of the office, make sure:

- you never leave items containing personal / sensitive (as defined at 2.4 above) information visible in your car
- personal / sensitive data stored on an electronic device (such as a laptop) is password protected and encrypted
- you only take the paperwork / equipment you need and lock it away out of sight in the boot of your car if you are not able to keep it with you
- you don't leave items containing personal / sensitive data overnight in your car.

**9.0 HANDLING / STORAGE / TRANSMISSION OF INFORMATION IN THE OFFICE**

9.1 Confidential information needs to be stored and handled in ways that limit access to those who have 'a need to know'.

9.2 Personal / special categories of personal data

9.2.1 Only access personal / special categories of personal data (whether held as paper records or electronically), if you are authorised by your line manager to do so.

**9.3 Paper records**

9.3.1 Make sure that records containing personal information are put away securely and never left lying around on desks or open to view in the organisation's premises. Careless handling of printed material could result in an unauthorised person being able to see it and read it.

9.3.2 If you are involved in printing documents containing personal information, make sure you do so securely. Do not leave printed material unattended in the printer, open to unauthorised viewing.

9.3.3 All paper records need to be stored in lockable, preferably fireproof cabinets / cupboards.

**9.4 Computer records**

9.4.1 Only access data held on computers if you are authorised by your line manager to do so.

9.4.2 Make sure your computer screen is turned away from public view and has appropriate shielding (such as a screen saver) so that no-one is able to casually view personal / special categories of personal data.

9.4.3 Personal / special categories of personal data stored on a computer or other electronic device needs to be password protected. If you need to write passwords down, make sure they are kept in a secure location within the office. Screen savers need also to be password protected.

9.5 There will be office processes in place regarding the following tasks:

- handling post
- sending and receiving emails
- accessing the internet
- using the fax machine.

If your job involves any of the above, you need to be familiar with these processes. If you are unsure about any aspects of the work you are doing, speak to your line manager.

## 10.0 RETENTION, ARCHIVING AND DISPOSAL OF INFORMATION

10.1 There are rules governing how long certain records and data must be kept and how they are to be disposed of once they pass their archiving date. Some rules are governed by different funders, SRCR will apply these appropriately.

10.2 Make sure you are familiar with the office processes that apply to the archiving and disposal of personal / sensitive data. This includes data held both electronically and in paper form.

10.3 Do not dispose of any personal / special categories of personal data if you are unsure of the rules that apply. If in doubt, ask your line manager.

## 11.0 PHOTOGRAPHS, AUDIO RECORDINGS AND VIDEO RECORDINGS

11.1 Photographs, audio recordings and video recordings in which an individual can be identified are classed as personal data and are subject to the same restrictions as all other personal data. This includes analogue and digital photographs (taken on cameras or mobile phones), film footage, CCTV footage or any other image.

11.2 You are not allowed to take or display photographs, audio recordings or video recordings of individual service users, unless your line manager and the person concerned have given you permission to do so.

11.3 Storage

11.3.1 If a photograph, audio recording or video recording is to be kept for re-use it will need to be stored securely either electronically or in hard copy format and only accessed by those people authorised to do so. Copies of the written consent for its use will need to be stored securely until all copies (both hard and electronic) of the actual photograph, audio recording or video recording have been destroyed.

## 12.0 USE OF SOCIAL NETWORKING

12.1 This includes such sites as Facebook, Twitter, YouTube (the list is not exhaustive). You need to be aware that by participating in social networking sites you could be in breach of:

- confidentiality and disclosure policy – for example by releasing confidential information (including photographs, audio recordings or video recordings) about identifiable individuals such as colleagues or service users without their permission
- codes of practice for health and social care workers in England and in Wales – for example by entering into inappropriate personal relationships with service users
- the organisation's code of conduct – for example by bringing trust in your professional role or the organisation into disrepute.

Any such breaches may result in disciplinary action under the disciplinary policy.

12.2 DO NOT, therefore:

- post any information (including photographs, audio recordings or video recordings) about service users, colleagues, project workers or any other persons with whom you come in to contact through work without the express permission of your line manager and the individual/s concerned
- post information (including photographs, audio recordings or video recordings) about yourself which may bring trust in your professional role or the organisation into disrepute
- post privileged information you may have about your employment (for example rates of pay, terms and conditions of employment)
- encourage or engage in cyber friendships with service users unless your line manager has approved it
- conduct any work-related activity, for example discussing / amending rotas or discussing care packages via social networking sites.

12.3 Social networking sites will only be used for work-related activity with the permission of your line manager on a case-by-case basis. Any such arrangements will be reviewed regularly.

## 13.0 TRANSFER / TRANSMISSION OF INFORMATION

13.1 The DPO / CG is required to ensure their organisation provides a statement on confidentiality to partner agencies, setting out the principles governing the sharing of information. This includes the expectation that the recipient undertakes to respect the need to maintain the confidentiality of the information shared.

13.2 Postal service

13.2.1 Confidential personal data sent by post will be marked “strictly private and confidential”, for attention of a named, designated individual only.

13.2.2 Managers will consider using a recorded delivery service when transferring personal data / special categories of personal data by post.

13.3 Fax

13.3.1 It is recommended that personal data / special categories of personal data are NOT transmitted by fax unless it is very urgent and the organisation has first established that there are adequate safeguards in place to protect confidentiality.

13.4 Internet

13.4.1 When accessing confidential information over the internet (for example accessing a care management package or financial information), managers will ensure reasonable technical security measures are in place and adhered to, in order to protect that data. These include ensuring that:

special provisions (such as data encryption) are in place to protect data being transmitted

computers are adequately protected with antivirus, antispyware, software and hardware firewalls

staff accessing the internet in a work-related capacity are trained in the potential threats that can emanate from it and how to manage them.

13.5 Email

13.5.1 When sending confidential information via email, managers need to have systems in place to ensure that:

where possible, the information is sent as a password protected attachment rather than in the body of an email

the destination address to which the information is to be transmitted has been checked
confirmation has been obtained in writing that the recipient of the information (for example the local authority) will handle it in strict confidence in line with the GDPR and that the information will not be used for purposes other than the one agreed
the information being sent is encrypted and password protected.

13.6 The GDPR provides that transfers of personal data outside of the European Economic Area (EEA) are prohibited unless there is adequate data protection in place. There are a number of conditions that must be met under the GDPR before a transfer outside of the EEA is deemed appropriate and legal advice should be sought if an international transfer is contemplated. In particular:
where the organisation uses cloud providers for the processing of personal information relating to any individual (staff or service user) it is important to obtain clarification from that provider as to the location of its computer servers
where a transfer is likely to result in a high risk to the rights of individuals, the organisation must, prior to the transfer, carry out a data protection impact assessment and appropriate contractual safeguards must be in place before the transfer proceeds.

## 14.0 LEARNING AND DEVELOPMENT

14.1 Your manager will assess the level of training you need depending on your role in the organisation.

14.2 Training will include all aspects of record keeping. If your job involves use of a computer system you will be trained in its use and in the data security implications of your work.

## 15.0 RESPONSIBILITIES OF MANAGERS

15.1 Managers are responsible for having safe and effective systems in place to ensure that:

- staff follow the data protection and subject access policy, procedure and guidance when handling service user data, in order to comply with the GDPR and the Caldicott Principles
- all data is collected, processed, maintained, stored, disclosed and disposed of in accordance with the Data Protection Principles and with the conditions for lawful processing as set out in the GDPR (see Appendix 3 and Appendix 4)
- fair processing information (known as a Privacy Notice) is issued to service users when collecting their personal data in accordance with the requirements set out in Appendix 5
- personal data / special categories of personal data are recorded accurately and kept only if relevant and justifiable
- personal records are properly managed, accurate, fit for purpose and remain confidential
- records are maintained demonstrating that the requirements imposed by the GDPR are being complied with, and how.

15.2 Managers are required to:

- nominate a Data Protection Officer / Caldicott Guardian (DPO / CG) and deputy
- ensure the nominated officers receive training in line with GDPR requirements and Caldicott Principles
- provide staff with contact details of the DPO / CG and deputy
- instruct staff to refer matters relating to data protection (including requests for subject access) to the DPO / CG or deputy.

15.3 Where personal data has been collected for direct marketing purposes, managers must

ensure they have permission from the person supplying the data to disclose it, before doing so.

- The original permission form must be checked to ensure it permits disclosure to the intended person/s or organisation.
- Direct marketing has a legal meaning. It does not just refer to activity with a commercial purpose but can cover any advertising, including the promotion of the aims or membership of the organisation.
- Special rules apply where direct marketing is carried out by phone, email and text message. Managers must ensure that any direct marketing by electronic means complies with the Information Commissioner's Direct Marketing Checklist, see https://ico.org.uk/media/for-organisations/documents/1551/direct-marketing-checklist.pdf).

15.4 When the organisation engages an external company to provide services on its behalf, (for example HR or IT services, off site storage or document disposal services) and is acting as a data processor for the purposes of GDPR, managers are responsible for ensuring that:

- the company is engaged by means of a written contract
- the company is able to provide sufficient guarantees as to the implementation of GDPR-compliant security measures
- the contract sets out the subject matter and duration of the processing, the nature and purposes of the processing, the type of personal data and categories of data subjects involved and includes the obligations and rights of the contracting organisation.

The contract must also include the additional obligations set out in Appendix 7.

## 16.0 TRUSTEE RESPONSIBILITIES

16.1 Trustees are required to familiarise themselves with the content of the data protection and subject access policy and to be aware of the associated procedure and guidance documents. The responsibility for having detailed knowledge of the procedure and guidance, and the monitoring of compliance to these documents within the organisation may be carried out by a nominated member of the board or delegated by them to an appropriate member of the management team.

16.2 Trustees are personally responsible for ensuring managers have safe and effective systems in place whereby staff work according to the data protection and subject access policy documents when handling personal and sensitive data.

## 17.0 ACCEPTANCE

17.1 You are required to sign to indicate that you have received, read and understood the content of this guidance as directed by your line manager and on completion of training it is your personal responsibility to follow it. Failure to do so may result in disciplinary proceedings.

## APPENDIX 1 DEFINITIONS

**Personal data**
This refers to any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal data can be:

- in written form, including email / text messages
- in the form of photographs / images in digital or analogue form, videos, CCTV footage or any other images
- audio recordings of voices.

**Special categories of personal data**
This is data covering racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic data, data concerning health or data concerning a natural person's sex life or sexual orientation.

The two categories of data above can apply to any individual and may include the following, though the list is not exhaustive:

- carers, family members and those with care needs
- employees
- volunteers
- trustees
- donors
- supporters
- people from other organisations
- members of other network partners within Carers Trust.

**Processing**
This refers to any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

**Data Controller**
This refers to an organisation or individual who (either jointly or in common with other organisations / individuals) determines the purposes for which and the manner in which any personal data are to be processed.

**Data Processor**
This refers to an organisation or individual (other than an employee of the data controller) who processes personal data on behalf of the data controller.

**Subject access**
This is a request from an individual to see information held on them.

**Third Party**
This refers to an individual or organisation who is not the data subject, not the data controller or employee of the data controller and not a data processor or employee of the data processor.

**Personal data breach**
This means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

**Data concerning health**
This refers to personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status

**Direct Marketing**
This refers to the communication (by whatever means) of any advertising or marketing material that is directed to particular individuals.

- It is not just restricted to marketing with a commercial or financial motive.
- It can include a charity contacting a data subject to notify them of a forthcoming profile-raising 'Open Day' for example, or it may include sending literature promoting or raising awareness of the non-profit-making aims and ideals of an organisation.
- Where the communication is made electronically by email, fax, telephone, text message the Privacy and Electronic Communications Regulations 2003 will apply.

**APPENDIX 2 CONSENT UNDER THE GDPR**

If relying on consent as a lawful basis for processing personal data under GDPR, then it must be freely given, specific, informed and unambiguous indication of the individual's wishes. This means there must be some form of clear affirmative action - or in other words a positive 'opt-in' - consent cannot be inferred from silence, pre-ticked boxes or inactivity.

Where consent is relied on as a condition for lawful processing, managers must ensure:

- consent is active, and does not rely on silence, inactivity or pre-ticked boxes
- consent to processing is distinguishable, clear, and is not *"bundled"* with other written agreements or declarations
- supply of services is not made contingent on consent to processing which is not necessary for the service being supplied
- data subjects are informed that they have the right to withdraw consent at any time (this will not affect the lawfulness of processing based on consent before its withdrawal)
- there are simple methods for withdrawing consent as there are for obtaining it
- separate consents are obtained for distinct processing operations
- consent is not relied on where there is a clear imbalance between the data subject and the controller (for example, where a service user does not have capacity).

Managers can rely on other lawful bases apart from consent, which may not always be appropriate, for example Article9(2)(h) of the GDPR, which legitimises processing for health and social care purposes.

**Children's Consent**
If the organisation offers an 'information society service' (that is, online services) to children, consent may need to be obtained from a parent or guardian to process the child's data.

The GDPR states that, if consent is the basis for processing the child's personal data, a child under the age of 16 cannot give that consent themselves and instead consent is required from a person holding 'parental responsibility' but it does permit member states to provide for a lower age in law, as long as it is not below 13 and we expect to see that age introduced under the Data Protection Bill.

'Information society services' includes most internet services provided at the user's request, normally for remuneration. The GDPR emphasises that protection is particularly significant where children's personal information is used for the purposes of marketing and creating online profiles.

Parental / guardian consent is not required where the processing is related to preventative or counselling services offered directly to a child.

**APPENDIX 3 PRINCIPLES OF THE GDPR**
These require personal data to be:

- processed lawfully, fairly, and in a transparent manner in relation to the data subject
- processed for limited, explicitly stated and legitimate purposes
- processed in a way that is adequate, relevant and limited to what is necessary for the purpose for which the data is collected and maintained
- accurate and where necessary kept up-to-date
- kept for no longer than is absolutely necessary
- kept safe and secure, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

The data controller is also required to be able to demonstrate how it is complying with the Data Protection Principles and its obligations under the GDPR.

CALDICOTT PRINCIPLES
These govern the use and management of patient-identifiable information within organisations providing regulated care and support services. In relation to patient-identifiable information, the organisation must:

- be able to justify the purpose of how they use and manage it
- not use such information unless it is necessary
- use the minimum necessary amount of information
- ensure it is accessed on a strict need-to-know basis
- ensure those accessing such information are aware of their responsibilities

- understand and comply with the law
- be aware that the need to share information can be as important as the duty to protect patient confidentiality.

For more information, visit:
https://en.wikipedia.org/wiki/Caldicott_Report#Caldicott_principles

**APPENDIX 4 LAWFUL PROCESSING UNDER GDPR**

For processing of personal data to be lawful under the GDPR, the DPO / CG needs to identify a lawful basis for doing so. This is often referred to as the "conditions for processing" and it is important that the lawful basis for processing personal data is determined and documented.

The tables below set out the lawful bases available for processing personal data and special categories of personal data.

Conditions for lawful processing under the GDPR: personal data (Article 6(1))
'Personal data can only be processed lawfully under the GDPR if one or more of the following are met:

(a) the data subject has consented to the processing;

(b) processing is necessary in order to enter into or perform a contract with the data subject;

(c) there is a legal obligation to perform the processing;

(d) it is necessary to protect the vital interests of the data subjects (this essentially applies in life or death scenarios);

(e) processing is necessary for the performance of a task carried out by a public authority or a private organisation acting in the public interest;

(f) processing is necessary because the controller or a third party has a legitimate interest in processing the data provided that the interest is not overridden by the rights or freedoms of the affected data subjects.

Conditions for lawful processing under the GDPR: special categories of personal data (Article 9(2))
'The processing of special categories of personal data (including data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic data, data concerning health or data concerning a natural person's sex life or sexual orientation) is prohibited unless one or more of the following apply:

(a) the data subject has given explicit consent;

(b) processing is necessary for the controller to comply with obligations or exercise rights in the context of employment, social security and social protection law;

(c) processing is necessary to protect vital interests of the data subject (or another person) where the data subject is incapable of giving advice;

(d) processing is carried out in the course of the legitimate activities of a charity or not-for-profit body, with respect to its own members, former members, or persons with whom it has regular contact in connection with its purposes

(e) processing relates to personal data which are manifestly made public by the data subject;

(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, and occurs on the basis of a law that is proportionate to the aim pursued and protects the rights of data subjects;

(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;

(i) processing is necessary for reasons of public interest in the area of public health;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to appropriate safeguards.'

**APPENDIX 5** FAIR PROCESSING INFORMATION

The GDPR includes detailed rules for giving what is commonly known as privacy information or privacy notices to data subjects in relation to the processing of their personal data.

The GDPR says that the information an organisation provides to people about how it processes their personal data must be:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.

The information should be provided at the time the data is obtained or as soon as possible thereafter (but at least within a month). It should be communicated in writing or by other means including where appropriate electronically for example through the organisation's website. If requested, it can be provided verbally provided that there is a record of communication and the identity of the data subject has been verified.

In particular, the information given will need to include the following:

- the contact details of the data controller (that is, the organisation)
- the contact details of the Data Protection Officer / CG and deputy

- the purposes of the processing for which the personal data are intended including the legal basis for processing (see Appendix 4)
- if the processing is based on legitimate interests pursued by the controller or a third party, an explanation of those interests
- data retention periods or reference to the criteria used to determine the retention period
- information on international transfers and safeguards applied to such transfers
- reference to the data subject's rights that is, right to request access to personal data and rectification or erasure, right to restrict or object to processing, right to data portability and complain to the Information Commissioner
- if the processing is based on consent, the right to withdraw consent at any time
- whether the provision of personal data is required as part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data
- the existence of automated decision making, including profiling and information about how decisions are made, the significance and consequences

The ICO has provided some guidance in its Privacy Notice Code of Practice, which contains general principles regarding the format and drafting style of privacy notices and broadly aligns with the GDPR.

**APPENDIX 6 KEEPING RECORDS FOR RESEARCH**

When a file's retention period has expired, it may be kept indefinitely for research or historical purposes subject to the following restrictions.

- The data will be rendered anonymous or will be pseudonymised if this is possible and does not diminish its research value.
- Researchers undertake to treat the data as confidential before being given access.
- Access will only be given for genuine research. The data will not be used to make decisions about particular individuals.
- Published research results must not refer to identifiable living individuals unless those individuals have been traced and have given consent. Where individuals have died, consent will need to be given by their next of kin.
- Where a researcher intends to contact individuals to collect additional material, prior consent will be obtained before the individuals are contacted.
- Where a file is not being kept for research or historical purposes, it will be securely destroyed along with corresponding electronic records.

**APPENDIX 7 CONTRACTS WITH EXTERNAL PROVIDERS**

The contract must include the following obligations on the provider:

- to process personal data only on written instructions from the organisation (including transfer of personal data outside the EEA) unless required to do so by UK or EU law;
- to immediately inform the organisation if it believes an instruction breaches the GDPR or any other UK or EU law;
- to ensure that anyone (including their employees) who is authorised to process personal data agrees to keep that personal data confidential or is under an appropriate statutory obligation of confidentiality;
- to take all measures required under the GDPR to ensure that they comply with the requirements around keeping personal data secure;
- not to engage a sub-contractor without (a) the organisation's prior specific or general written authorisation; (b) ensure the same contractual obligations are imposed on that sub-contractor and (c) to be responsible and liable to the organisation if the sub-

processor fails to perform its obligations;

- to implement appropriate measures to assist the organisation to discharge its obligations in respect of data subjects and their rights, including responding to subject access requests;
- to assist the organisation in complying with its obligations around security, notification of security breaches and data protection impact assessments;
- at the discretion of the organisation to delete, or return all personal data after the end of the contract and to delete existing copies unless UK law requires storage of the personal data;
- to make available to the organisation all information necessary to demonstrate compliance with their obligations under the GDPR and allow (and contribute to) audits conducted by the organisation or another auditor appointed on the organisation's behalf;
- to maintain a record of its processing activities in accordance with the GDPR; and
- appoint a DPO where appropriate.

The contracting organisation may wish to seek legal advice to ensure service contracts are GDPR compliant and contain appropriate safeguards.

This guidance was accepted by the Board of Trustees on 17th May 2018

Date for review: May 2021