Data Protection / GDPR Policy

Date reviewed:	October 2025
Date due for review:	October 2028 or as and when required
Date of Trustee approval:	November 2025
To be reviewed by:	Head of Operations

1 Introduction

York CVS is committed to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with all our legal obligations.

We hold personal data about our employees, trustees, consultants, volunteers, clients, suppliers and other individuals for a variety of business purposes.

This policy sets out how we seek to protect personal data and ensure that our staff and volunteers understand the rules governing their use of the personal data to which they have access during their work.

This policy requires staff to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

2 Definitions

2.1 Business Purposes

Business purposes include the following: -

- Personnel, administrative, financial, regulatory, payroll and business development purposes
- Compliance with our legal, regulatory and corporate governance obligations and good practice
- Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests
- Ensuring business policies are adhered to (such as policies covering email and internet use)
- Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking
- Investigating complaints
- Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments
- Monitoring staff conduct and human resource management matters
- Marketing our business - improving services.

2.2 Personal data

'Personal data' means 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 we gather may include: individuals' phone number, email address, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.

2.3 Special categories of personal data

Special categories of data include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings, and genetic and biometric information - any use of special categories of personal data should be strictly controlled in accordance with this policy.

2.4 Data controller

'Data controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law.

2.5 Data processor

'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

2.6 Processing

'Processing' means 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.

2.7 Supervisory authority

This is the national body responsible for data protection. The supervisory authority for our organisation is the Information Commissioners Office.

3 Scope

This policy applies to all staff, volunteers, trustees and freelance consultants who must be familiar with this policy and comply with its terms.

This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

4 Who is responsible for this policy?

As our Data Protection Officer (DPO), Lisa Egginton has overall responsibility for the day-to-day implementation of this policy. You should contact the DPO for further information about this policy if necessary. lisa.egginton@yorkcvs.org.uk

5 The Principles

York CVS shall comply with the principles of data protection (the Principles) enumerated in the Data Protection Act 2018. We will make every effort possible in everything we do to comply with these principles.

The Principles are:

1. *Lawful, fair and transparent*

Data collection must be fair, for a legal purpose and we must be open and transparent as to how the data will be used.

2. *Limited for its purpose*

Data can only be collected for a specific purpose.

3. *Data minimisation*

Any data collected must be necessary and not excessive for its purpose.

4. *Accurate*

The data we hold must be accurate and kept up-to-date.

5. *Retention*

We cannot store data longer than necessary.

6. *Integrity and confidentiality*

The data we hold must be kept safe and secure.

6 Accountability and transparency

We must ensure accountability and transparency in all our use of personal data. We must show how we comply with each Principle. You are responsible for keeping a written record of how all the data processing activities you are responsible for comply with each of the Principles. This must be kept up-to-date and must be approved by the DPO.

To comply with data protection laws and the accountability and transparency Principle of GDPR, we must demonstrate compliance. You are responsible for understanding your responsibilities to ensure we meet the following data protection obligations:

- Fully implement all appropriate technical and organisational measures

- Maintain up-to-date and relevant documentation on all processing activities
- Conducting Data Protection Impact Assessments
- Implement measures to ensure privacy by design and default, including:
    - Data minimisation
    - Pseudonymisation
    - Transparency
    - Allowing individuals to monitor processing
    - Creating and improving security and enhanced privacy procedures on an ongoing basis.

7 Our Procedures

7.1 Fair and lawful processing

We must process personal data fairly and lawfully in accordance with individuals' rights under the first Principle. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

If we cannot apply a lawful basis (explained below), our processing does not conform to the first principle and will be unlawful. Data subjects have the right to have any data unlawfully processed erased.

7.2 Controlling vs. processing data

York CVS is classified as a data controller and data processor. We must maintain our appropriate registration with the Information Commissioners Office to continue lawfully controlling and processing data.

7.3 For data processors

As a data processor, we must comply with our contractual obligations and act only on the documented instructions of the data controller. If we at any point determine the purpose and means of processing out with the instructions of the controller, we shall be considered a data controller and therefore breach our contract with the controller and have the same liability as the controller.

As a data processor, we must:

- Not use a sub-processor without written authorisation of the data controller
- Co-operate fully with the ICO or other supervisory authority
- Ensure the security of the processing
- Keep accurate records of processing activities
- Notify the controller of any personal data breaches.

If you are in any doubt about how we handle data, contact the DPO for clarification.

7.4 Lawful basis for processing data

We must establish a lawful basis for processing data. Ensure that any data you are responsible for managing has a written lawful basis approved by the DPO. It is your responsibility to check the lawful basis for any data you are working with and ensure all your actions comply the lawful basis. At least one of the following conditions must apply whenever we process personal data:

1. *Consent*

We hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose.

2. *Contract*

The processing is necessary to fulfil or prepare a contract for the individual.

3. *Legal obligation*

We have a legal obligation to process the data (excluding a contract).

4. *Vital interests*

Processing the data is necessary to protect a person's life or in a medical situation.

5. *Public function*

Processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law.

6. *Legitimate interest*

The processing is necessary for our legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest.

8 Deciding which condition to rely on

If you are assessing the lawful basis, you must first establish that the processing is necessary. This means the processing must be a targeted, appropriate way of achieving the stated purpose. You cannot rely on a lawful basis if you can reasonably achieve the same purpose by some other means.

Remember that more than one basis may apply, and you should rely on what will best fit the purpose, not what is easiest.

Consider the following factors and document your answers:

- What is the purpose for processing the data?
- Can it reasonably be done in a different way?

- Is there a choice as to whether to process the data?
- Who does the processing benefit?
- After selecting the lawful basis, is this the same as the lawful basis the data subject would expect?
- What is the impact of the processing on the individual?
- Are you in a position of power over them?
- Are they a vulnerable person?
- Would they be likely to object to the processing?
- Are you able to stop the processing at any time on request, and have you factored in how to do this?

Our commitment to the first Principle requires us to document this process and show that we have considered which lawful basis best applies to each processing purpose, and fully justify these decisions.

We must also ensure that individuals whose data is being processed by us are informed of the lawful basis for processing their data, as well as the intended purpose. This should occur via a privacy notice. This applies whether we have collected the data directly from the individual, or from another source.

If you are responsible for assessing the lawful basis and implementing the privacy notice for the processing activity, you must complete a Projects Declaration Form and share this with the DPO.

9 Special categories of personal data

What are special categories of personal data?

Previously known as sensitive personal data, this means data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual's:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sexual orientation.

In most cases where we process special categories of personal data we will require the data subject's explicit consent to do this unless exceptional circumstances apply, or we are required to do this by law (e.g. to comply with legal obligations to ensure

health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

The condition for processing special categories of personal data must comply with the law. If we do not have a lawful basis for processing special categories of data that processing activity must cease.

10 Responsibilities

10.1 Our responsibilities

- Analysing and documenting the type of personal data we hold
- Checking procedures to ensure they cover all the rights of the individual
- Identify the lawful basis for processing data
- Ensuring consent procedures are lawful
- Implementing and reviewing procedures to detect, report and investigate personal data breaches
- Store data in safe and secure ways
- Assess the risk that could be posed to individual rights and freedoms should data be compromised.

10.2 Your responsibilities

- Fully understand your data protection obligations
- Check that any data processing activities you are dealing with comply with our policy and are justified
- Do not use data in any unlawful way
- Do not store data incorrectly, be careless with it or otherwise cause us to breach data protection laws and our policies through your actions
- Comply with this policy always
- Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay.

10.3 Responsibilities of the Data Protection Officer

- Keeping the board updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all staff members and those included in this policy
- Answering questions on data protection from staff, board members and other stakeholders
- Responding to individuals such as clients and employees who wish to know which data is being held on them by us
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing.

10.4 Responsibilities of the Operations Manager

- Ensure all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party services, such as cloud services the company is considering using to store or process data.

10.5 Responsibilities of the Communications and Engagement Office

- Approving data protection statements attached to emails and other marketing copy
- Addressing data protection queries from clients, target audiences or media outlets
- Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy.

11 Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DPO.

12 Data security

You must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

13 Storing data securely

In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it:

- Printed data should be shredded when it is no longer needed
- Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all staff to use a password manager to create and store their passwords.
- Data stored on CDs or memory sticks must be encrypted or password protected and locked away securely when they are not being used
- The DPO must approve any cloud used to store data

- Servers containing personal data must be kept in a secure location, away from general office space
- Data should be regularly backed up in line with the company's backup procedures
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones
- All servers containing sensitive data must be approved and protected by security software
- All possible technical measures must be put in place to keep data secure.

14 Data retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, considering the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

15 Transferring data internationally

There are restrictions on international transfers of personal data. You must not transfer personal data abroad, or anywhere else outside of normal rules and procedures without express permission from the DPO.

16 Rights of individuals

Individuals have rights to their data which we must respect and comply with to the best of our ability. We must ensure individuals can exercise their rights in the following ways:

1. *Right to be informed*

- Providing privacy notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language, particularly if aimed at children.
- Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

2. *Right of access*

- Enabling individuals to access their personal data and supplementary information.
- Allowing individuals to be aware of and verify the lawfulness of the processing activities.

3. *Right to rectification*

- We must rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete.

- This must be done without delay, and no later than one month. This can be extended to two months with permission from the DPO.

4. *Right to erasure*

- We must delete or remove an individual's data if requested and there is no compelling reason for its continued processing.

5. *Right to restrict processing*

- We must comply with any request to restrict, block, or otherwise suppress the processing of personal data.
- We are permitted to store personal data if it has been restricted, but not process it further. We must retain enough data to ensure the right to restriction is respected in the future.

6. *Right to data portability*

- We must provide individuals with their data so that they can reuse it for their own purposes or across different services.
- We must provide it in a commonly used, machine-readable format, and send it directly to another controller if requested.

7. *Right to object*

- We must respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.
- We must respect the right of an individual to object to direct marketing, including profiling.
- We must respect the right of an individual to object to processing their data for scientific and historical research and statistics.

8. *Rights in relation to automated decision making and profiling*

- We must respect the rights of individuals in relation to automated decision making and profiling.
- Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

17 Privacy notices

17.1 When to supply a privacy notice

A privacy notice must be supplied at the time the data is obtained if obtained directly from the data subject. If the data is not obtained directly from the data subject, the privacy notice must be provided within a reasonable period of having obtained the data, which mean within one month.

If the data is being used to communicate with the individual, then the privacy notice must be supplied at the latest when the first communication takes place.

If disclosure to another recipient is envisaged, then the privacy notice must be supplied prior to the data being disclosed.

17.2 What to include in a privacy notice

Privacy notices must be concise, transparent, intelligible and easily accessible. They are provided free of charge and must be written in clear and plain language, particularly if aimed at children.

The following information must be included in a privacy notice to all data subjects:

- Identification and contact information of the data controller and the data protection officer
- The purpose of processing the data and the lawful basis for doing so
- The legitimate interests of the controller or third party, if applicable
- The right to withdraw consent at any time, if applicable
- The category of the personal data (only for data not obtained directly from the data subject)
- Any recipient or categories of recipients of the personal data
- Detailed information of any transfers to third countries and safeguards in place
- The retention period of the data or the criteria used to determine the retention period, including details for the data disposal after the retention period
- The right to lodge a complaint with the ICO, and internal complaint procedures
- The source of the personal data, and whether it came from publicly available sources (only for data not obtained directly from the data subject)
- Any existence of automated decision making, including profiling and information about how those decisions are made, their significances and consequences to the data subject.
- Whether the provision of personal data is part of a statutory of contractual requirement or obligation and possible consequences for any failure to provide the data (only for data obtained directly from the data subject).

18 Subject Access Requests

18.1 What is a subject access request?

An individual has the right to receive confirmation that their data is being processed, access to their personal data and supplementary information which means the information which should be provided in a privacy notice.

18.2 How we deal with subject access requests

Please refer any subject access requests to the DPO in the first instance. We must provide an individual with a copy of the information the request, free of charge. This must occur without delay, and within one month of receipt. We endeavour to provide

data subjects access to their information in commonly used electronic formats, and where possible, provide direct access to the information through a remote accessed secure system.

If complying with the request is complex or numerous, the deadline can be extended by two months, but the individual must be informed within one month. You must obtain approval from the DPO before extending the deadline.

We can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, we can request the individual specify the information they are requesting. This can only be done with express permission from the DPO.

Once a subject access request has been made, you must not change or amend any of the data that has been requested. Doing so is a criminal offence.

19 Data portability requests

We must provide the data requested in a structured, commonly used and machine-readable format. This would normally be a CSV file, although other formats are acceptable. We must provide this data either to the individual who has requested it, or to the data controller they have requested it be sent to. This must be done free of charge and without delay, and no later than one month. This can be extended to two months for complex or numerous requests, but the individual must be informed of the extension within one month and you must receive express permission from the DPO first.

20 Right to erasure

20.1 What is the right to erasure?

Individuals have a right to have their data erased and for processing to cease in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and / or processed
- Where consent is withdrawn
- Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed or otherwise breached data protection laws
- To comply with a legal obligation
- The processing relates to a child.

20.2 How we deal with the right to erasure

We can only refuse to comply with a right to erasure in the following circumstances:

- To exercise the right of freedom of expression and information

- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims.

If personal data that needs to be erased has been passed onto other parties or recipients, they must be contacted and informed of their obligation to erase the data. If the individual asks, we must inform them of those recipients.

21 The right to object

Individuals have the right to object to their data being used on grounds relating to their situation. We must cease processing unless:

- We have legitimate grounds for processing which override the interests, rights and freedoms of the individual.
- The processing relates to the establishment, exercise or defence of legal claims.

We must always inform the individual of their right to object at the first point of communication, i.e. in the privacy notice. We must offer a way for individuals to object online.

22 The right to restrict automated profiling or decision making

We may only carry out automated profiling or decision making that has a legal or similarly significant effect on an individual in the following circumstances:

- It is necessary for the entry into or performance of a contract
- Based on the individual's explicit consent
- Otherwise authorised by law.

In these circumstances, we must:

- Give individuals detailed information about the automated processing.
- Offer simple ways for them to request human intervention or challenge any decision about them.
- Carry out regular checks and user testing to ensure our systems are working as intended.

23 Third parties

23.1 Using third party controllers and processors

As a data controller and data processor, we must have written contracts in place with any third party data controllers and data processors that we use. The contract must

contain specific clauses which set out our and their liabilities, obligations and responsibilities.

23.2 For controllers

As a data controller, we must only appoint processors who can provide sufficient guarantees under GDPR and that the rights of data subjects will be respected and protected.

23.3 For processors

As a data processor, we must only act on the documented instructions of a controller. We acknowledge our responsibilities as a data processor under GDPR and we will protect and respect the rights of data subjects.

24 Contracts

Our contracts must comply with the standards set out by the ICO and, where possible, follow the standard contractual clauses which are available. Our contracts with data controllers and data processors must set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller.

At a minimum, our contracts must include terms that specify:

- Acting only on written instructions
- Those involved in processing the data are subject to a duty of confidence
- Appropriate measures will be taken to ensure the security of the processing
- Sub-processors will only be engaged with the prior consent of the controller and under a written contract
- The controller will assist the processor in dealing with subject access requests and allowing data subjects to exercise their rights under GDPR
- The processor will assist the controller in meeting its GDPR obligations in relation to the security of processing, notification of data breaches and implementation of Data Protection Impact Assessments
- Delete or return all personal data at the end of the contract
- Submit to regular audits and inspections and provide whatever information necessary for the controller and processor to meet their legal obligations.
- Nothing will be done by either the controller or processor to infringe on GDPR.

25 Criminal offence data

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject. We cannot keep a comprehensive register of criminal offence data. All data relating to criminal offences is a special category of personal data and must be treated as such. You must have approval from the DPO prior to carrying out a criminal record check.

26 Audits, monitoring and training

26.1 Data audits

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant. You must conduct a regular data audit as defined by the DPO and normal procedures.

26.2 Monitoring

Everyone must observe this policy. The DPO has overall responsibility for this policy. York CVS will keep this policy under review and amend or change it as required. You must notify the DPO of any breaches of this policy. You must comply with this policy fully and always.

26.3 Training

You will receive adequate training on provisions of data protection law specific for your role. You must complete all training as requested. If you move role or responsibilities, you are responsible for requesting new data protection training relevant to your new role or responsibilities.

If you require additional training on data protection matters, contact the DPO.

27 Reporting breaches

Any breach of this policy or of data protection laws must be reported as soon as practically possible. This means as soon as you have become aware of a breach. York CVS has a legal obligation to report any data breaches to the Information Commissioner within 72 hours.

All members of staff have an obligation to report to the DPO actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the ICO of any compliance failures that are material either or as part of a pattern of failures.

Any member of staff who fails to notify of a breach or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.

28 Failure to comply

We take compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

29 Appendix A: Data storage and retention

The fifth principle of the Data Protection Act states that 'personal data kept for any purpose shouldn't be kept for longer than necessary'.

All paper files and documents should be scanned on to SharePoint and shredded.

Type of data	Retention Period	Reason	Where is the data kept
Application forms and interview notes (for unsuccessful candidates)	6 months after recruitment	Provision for challenges and/or course cases	SharePoint; HR; Recruitment
Personnel files and training records	7 years after employment ceases	Provision of references and time limit for court cases	SharePoint; HR; Personnel files; name
Facts relating to redundancies	12 years from date of redundancy	Limitation period for litigation	SharePoint; HR; Redundancies
Income Tax and NI Returns	7 years after the financial year to which they refer	Tax regulations 1993	SharePoint; Finance
Statutory Maternity Pay calculations/records	7 years after the financial year to which they refer	Maternity Pay regulations 1986	SharePoint; Finance
Records and accident reports	3 years after date of the last entry (in the case of a child, records should be kept for 21 years)	RIDDOR 1985	SharePoint; SMT; Accidents and Incidents
Health records	During employment	Management of Health & Safety regulations	SharePoint; HR Personnel files; name
Health Records leading to termination of employment	7 years after employment ceases	Time limit for personal injury claims	SharePoint ; HR; Archived Personnel files; name
Medical Records kept because of Control of Hazardous Substances	40 years	COSHHR 1994	SharePoint ; H&S; Medical records (hazardous substances)

30 Appendix B: For more information

Useful external contacts

Information Commissioner
https://ico.org.uk/

https://ico.org.uk/for-organisations/data-protection-reform/

Gov.UK have several pages devoted to Data Protection laws and allied regulations
https://www.gov.uk/data-protection/the-data-protection-act

ACAS guidance linking workplace issues and employment law to the Data Protection Act.
http://www.acas.org.uk/index.aspx?articleid=3717

For Healthwatch England
https://www.healthwatch.co.uk/privacy