DATA PROTECTION POLICY

Policy Type:	BOARD
Policy Area:	Corporate
Policy Number:	8c V5
Produced by:	Chief Finance Officer (CFO)
Scrutinised by the Health and Safety Committee:	13 May 2025
Reviewed externally:	19 May 2025 by Risk Evolves
Approved by the Board:	28 May 2025
Issued Date	2 June 2025 To all staff for signing via People HR
Review Date:	May 2027

CONTENTS

1 Introduction

1.1 YMCA Black Country Group ("YMCABCG") is a 'data controller' or a 'data processor' depending on the nature of the relationship with the data subject, e.g. YMCABCG is a data controller in relation to our employees and other stakeholders such as those we provide housing for and those attending our nurseries. When information is shared with us from other parties such as Social Care teams or Health Care Providers, we may be the data processor of that data. The nature of the relationship will define the designation of controller or processor

1.2 In order to operate efficiently, YMCA Black Country Group has to collect and use certain types of data and information about people with whom it works. This includes current and past residents and service users, current and past employees, volunteers, suppliers, donors and others with whom it communicates. In addition, it may be required by law to collect and use certain types of information in order to comply with the requirements of statutory and regulatory bodies. This personal information must be dealt with and maintained in a proper manner, whether it be on paper, computerised records or recorded on other material.

This document has been created to outline and highlight YMCABCG compliance with data protection law, including the UK Data Protection Act 2018 (DPA) and the UK General Data Protection Regulation.

1.3 YMCABCG is fully committed to comply with the requirements of the Data Protection Act 2018 ("**the Act**"), which came into force on 25th May 2018. This policy has been prepared in accordance with its requirements, along with the following legislation, regulations and codes of practice:

- Data Protection Regulations (Fundamental Rights and Freedoms) Regulations 2023
- UK General Data Protection Regulation (UK GDPR)
- Privacy and Electronic Communications Regulations 2003
- The Freedom of Information Act 2000
- Computer Misuse Act 1990
- Human Rights Act 1998
- Common law duty of confidentiality
- Digital Economy Act
- Environmental Information Regulations (2004)
- Surveillance Camera Code of Practice
- Data Sharing Code of Practice

1.4 **The Act** gives protection to individuals about how data is recorded either manually or electronically. Individuals have a right of access to information held about them and may challenge this information if they feel it is inaccurate or has caused damage to them. **The Act** places obligations on those who record and use information about individuals.

1.5 It is important that as employees and volunteers of YMCABCG we are aware of the legislation governing data storage and use and strive to fully adhere to the principles set out in **the Act**.

1.6 In addition, YMCABCG will register, and keep up to date with the renewals with the Information Commissioner's Office. Our registration number is: Z9943063

1.7 This Policy applies to all YMCA Black Country Group members, current and former employees, volunteers, contractors, apprentices and consultants, including our subsidiaries and associated companies.

1.8 This Policy is to be read in conjunction with YMCCABCG's:

- Disciplinary Procedures;

- Staff Handbook; and
- Whistleblowing Policy.
- Privacy Notice
- and any other notices we issue to you from time to time in relation to personal data.

This policy does not form part of your contract of employment (or contract for services if relevant) and can be amended by YMCABCG at any time.

Any breach of this policy may result in disciplinary action being taken up to and including dismissal.

2 Scope

2.1 YMCABCG will ensure that the organisation treats personal information lawfully and correctly.

2.2 YMCABCG will comply with the seven data protection principles per the Data Protection Act which requires that personal data shall be:

a) Processed lawfully, fairly and in a transparent manner in relation to individuals;
b) Collected for a specific, explicit and legitimate purpose and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical shall not be considered to be incompatible with the initial purposes;
c) Adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed;
d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by GDPR in order to safeguard the rights and freedoms of individuals;
f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures; and
g) The Controller shall be accountable for and be able to demonstrate compliance with a) to f) above.

2.3 How we define processing

'Processing' means any operation which is performed on personal data such as:

- Collection, recording, organisation, structuring or storage
- Adaption or alteration
- Retrieval, consultation or use
- Disclosure by transmission, dissemination or otherwise making available
- Alignment or combination and
- Restriction, destruction or erasure.

This includes processing personal data which forms part of a filing system and any automated processing.

2.4 How and Why, We Process Personal Data

'Processing' the data that we hold includes collection, recording, organisation, structuring or storage, adapting, retrieving, disseminating, aligning and also removing or erasing it.

When we process personal data, we must have a lawful basis for doing so. The DPA 2018 identifies the six legal reasons for which data can be used by an organisation, including the conditions for the processing of special category data.

These include:

- Consent – the data subject is given the option to agree (or not) to the processing
- Performance of Contract (to perform a task) – processing where the data is necessary to fulfil a task that the data subject is requesting
- Legal Obligation – processing of personal data as stipulated by legal requirements. For example, employee personal data shared with HMRC or the Charity Commission.
- Vital Interest – processing necessary for the health or wellbeing of the data subject. For example, to seek urgent medical attention where a persons' life may be endangered
- Public Task - Where it is needed in the public interest or for official purposes
- Legitimate Interest – this is processing that is in both the interest of the organisation and the person. We must be able to demonstrate that the person would be genuinely interested and ensure that the processing is fair and balanced i.e. not just in our interest. This is commonly used for processing activities such as sending greeting cards or marketing

3 Roles and Responsibilities

3.1 All YMCABCG staff and Trustees will be involved and have an important part to play in the identification and management of risk.

3.2 Specific responsibilities have been allocated as follows:

Department/Area	**Role/Responsibility**
Board of Trustees	Board is responsible for: a. overseeing the effectiveness of the Data Protection Policy. b. monitoring compliance against the requirements of the Data Protection Policy. c. requiring the provision of reports on specific Data Protection risk identified.
Health and Safety Committee	The Health and Safety Committee is responsible for: a. requiring the provision of reports on the performance of systems used to identify and manage Data Protection Issues regularly reviewing these reports. b. Request additional reports be prepared by the Chief Officer Team as required to provide assurance in relation to Data Protection issues c. Scrutinise the Data Protection Policy as required by the Policy prior to recommending the Register be approved by the Board

Chief Executive Officer	Written permission of the **Chief Executive Officer** is required where information is considered exempt for disclosure in relation to Subject Data Requests.
Data Protection Officer	The **Data Protection Officer** is the CFO a) to inform and advise YMCCABCG and our employees about our obligations to comply with the UK GDPR and other data protection laws; b) to monitor compliance with the UK GDPR and other data protection laws, and with our data protection polices, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits; c) to advise on, and to monitor, data protection impact assessments; d) to cooperate with the ICO; and e) to be the first point of contact for the ICO.
HR Team	The HR Team is responsible for overseeing the processing of data rights requests
Employees (temporary or permanent), volunteers, contractors, agents and anyone else processing information on our behalf	All staff have a duty to protect personal data / personal information as set out below: a. Not to disclose personal data to anybody internal or external to the organisation who doesn't need to know. b. not to leave the desktop of their PC/laptop/mobile device unlocked when unattended. c. Change their passwords when prompted to do so and keep these passwords secure from internal colleagues and external sources. d. Not allow unauthorised persons to view screen e. Not leave computer print outs containing personal data/information in the printer, on their desk or in an unlocked drawer f. Not use data for a purpose other than that stated on service user registration. g. Keep all files, documents and information containing personal data, paper or electronic, secure. h. Not to use USB sticks or other removable media to store personal data. If needing to access documents from another PC/Laptop/Mobile device, SharePoint must be used. i. Not make subjective statements/statements of opinion on service user records

4 Personal Data

4.1 The Data Protection Act 2018 applies only to information that constitutes "personal data."

4.2 Information is "personal data" if it identifies a person, whether by itself, or together with information in the organisation's possession, or is likely to come into its possession; and is about a living person and affects that person's privacy (whether in his / her personal or family life, business or professional capacity) in the sense that the information has the person as its focus or is otherwise biological in nature.

4.3 Personal data covers both factual information and opinions about an individual.

4.4 YMCABCG may process a lot of wide-ranging personal information relating to its customers, their families and other during its day-to-day operations. This personal data may include names and addresses, bank details, academic, disciplinary, admissions, adoption and attendance records amongst other things.

4.5 This personal data might be provided to us by the data subject, or someone else (such as a family member, an advocate, doctor or physician, or an agency, or it could be created by us. It could be provided or created during an application process for housing, a recruitment process or during the contract of employment (or services) or after its termination.

4.6 The types of personal data we collect, and use, is documented in the appropriate Privacy Notice.

5 Special Category and Sensitive Data

5.1 **"The Act"** identifies categories of data. Some personal data that is processed will be of a higher risk if we were to compromise or list the data and in particular, would be more damaging to the rights and freedoms of individuals. This data is defined as **"special category data"** and includes the following information:

a) Ethnic or racial origin
b) Political opinion
c) Religious beliefs
d) Philosophical beliefs
e) Trade Union membership
f) Bio-metric data e.g. fingerprints, retinal scans
g) Medical information
h) Sex life
i) Sexual orientation

5.2 Additionally, as a Charity, we will also process other data that whilst is not defined as special category data within the definition of **"The Act"** would still be damaging to YMCABCG should the data be compromised. This data will include bank account details, payment card information and financial records.

5.3 In both cases of special category or sensitive data, the manner in which we process data must be treated with higher degrees of security and protection; and in many cases only with the explicit consent of the person whose data it belongs. For example, the processing of special category data is prohibited unless certain conditions are met e.g. consent from the data subject or processing is required to meet a certain obligation.

6 Collection and Handling of Personal/Special Category / Sensitive Data

6.1 YMCABCG will, through appropriate controls, management and review:

- Observe fully conditions regarding the fair collection and use of personal information.
- Meet its legal obligations to specify the purpose for which the information is used.
- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with legal requirements.
- Ensure the quality of information used.
- Apply strict checks to determine length of time information is held and destroy the data when this period has elapsed.
- Retain personal data for no longer than is necessary in accordance with Principle 5 of **the Act.**
- Take all appropriate technical and organisational security measures to safeguard personal information.
- Ensure that personal information is not transmitted outside the UK without suitable safeguards.
- Ensure the rights of people about whom the information is held can be fully exercised under **the Act**.

6.2 In addition, YMCABCG will ensure:

- There is a specific named person within the Association with responsibility for data protection.
- All staff and volunteers and other parties who handle personal information are aware of their personal responsibilities and wider organisational responsibilities for following good data protection practice.
- All staff and volunteers and other parties handling personal information is appropriately trained to do so.
- All staff and volunteers and other parties managing and handling personal information is appropriately supervised.
- Staff and volunteers and other parties are aware of the processes in place to deal with an enquiry about the handling of personal data.
- Any queries regarding the handling of personal data are dealt with promptly and courteously.
- Methods of handling and storing personal information are regularly assessed and evaluated.
- Performance with handling personal information is regularly assessed and evaluated.
- Any data sharing is carried out under written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.
- Any personal data / information destroyed is only done so in accordance with Section 12 "Data Destruction"

6.3 All managers, staff and appropriate volunteers within the Association will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss and/or disclosure. Staff will utilise Multi-Factor Authentication (MFA) to access corporate systems including E-Mail.

6.4 It is the responsibility of the appropriate manager to ensure that their team is made fully aware of this policy and their duties and responsibilities.

6.5 All contractors, consultants, partners and other agents of YMCABCG must ensure that they and all of their staff who have access to personal data held or processed for or on behalf of the Association, are aware of this policy and fully trained in and aware of their duties and responsibilities under **the Act**. Any breach will be deemed as breach of contract or agreement between YMCABCG and that individual, company, partner or firm.

7 CCTV

7.1 The use of CCTV systems are utilised across YMCABCG's sites for the purpose of service user, staff and public safety and to ensure site security. The same legally enforceable information handling processes of personal data and CCTV images shall be adhered to.

7.2 In terms of CCTV, YMCABCG images are kept for between 14 and 28 days depending upon the DVR's capacity. If a crime is reported to Police or there has been a serious incident or accident, images will be copied and retained until Police, or our insurers have had time to collect them.

7.3 Where CCTV is in operation, signs will be displayed, and the data processing will be included in the appropriate Privacy notice.

YMCABCG ensures the safe handling of CCTV images in accordance with the handling of personal data outlined under **the Act** and the requirements laid out by the Biometrics and Surveillance Camera Commissioner and the Surveillance Camera Code of Practice

8 Computer Use, Electronic Communications and Wireless Internet Connections

8.1 Under no circumstances should staff or volunteers of the Association attempt to connect to the Association's email system, files or databases using any publicly accessible device – this includes shared usage personal devices. If personal devices are used these must be virus protected using up-to-date software, use a separate password protected user account to prevent unauthorised access and encrypted to secure data in the event of loss or theft. The Association has the right to require such personal devices be provided for inspection if requested. Normally personal devices have minimal security and can be easily hacked, resulting in a breach of **the Act.**

8.2 Under no circumstances should staff or volunteers of the Association allow anyone else, including partners, friends and family members, to use a device supplied by the Association either for personal use or to access the Association's email system, files or databases on their behalf, or access any organisational data or systems on your personal devices.

8.3 We recognise that staff or volunteers may need to access their email, files or databases when not connected to the YMCABCG network including public networks. This is only permissible provided that a device is supplied by the Association or a personal device protected as described in 8.1 above is used. When using public networks you must only access the Association's M365 email system, SharePoint, OneDrive, File Server using MFA (set by default) and the housing application Active-H via the Site to Site Virtual Private Network (VPN) Microsoft client using.

8.4 Under no circumstances must you leave either a device supplied by the Association or a personal device unattended at any time, including whilst working remotely or using public networks.

8.5 It is the responsibility of the device user/owner to ensure that passwords are such that they cannot be easily compromised and are not recorded where they may be seen or accessed by anyone else who could jeopardise the security of YMCABCG.

8.6 Staff and volunteers of the Association must ensure that they are not breaching any data protection when they write and send emails. This could include (but is not limited to):

- Passing on personal information about an individual or third party without their consent
- Passing on any sensitive personal information
- Keeping personal information longer than necessary
- Sending personal information to a country outside the UK

8.7 Email correspondence will be avoided when transmitting personal data about a third party. Any email containing personal information about an individual may be liable to disclosure to the individual under the Act; this includes comments and opinion, as well as factual information. All staff must consider this when writing emails, and when keeping them.

9 Acceptable use of artificial intelligence (A.I.)

Artificial Intelligence (AI) has emerged as a transformative force in the business landscape, revolutionising various industries and sectors with its wide-ranging applications. Ensuring the acceptable and controlled use of AI is vital to maintain quality of output, ethical standards and trust with clients.

Evaluation and authorisation of A.I use. Before integration and implementation, all AI tools and systems used are evaluated and authorised by the IT Provider, CEO and the DPO depending on context and subject expertise.

The AI systems and tools currently used for operations within are documented in the Assets Register and Approved Software List.

AI added in a later patch.

As the AI technology matures more and more software and equipment will start to use it. It will be expected that systems initially evaluated and introduced into the organisations ecosystem without AI capability may have it introduced in a later patch update etc. Employees are encouraged to stay vigilant of these changes and report them to us before further use so the capability can be reevaluated.

Types of A.I

Employees are to be aware that although certain AI tools have been authorised for use within the organisation, these tools must be evaluated for suitability and legality before being used, especially for the processing of sensitive and special category data.

Descriptions of AI that could be useful to us

a) **Generative AI.** Generative AI technologies, such as natural language processing and image generation algorithms, are becoming increasingly adept at creating human-like content. While these innovations can streamline document production and enhance efficiency, Employees must remain vigilant in ensuring that generated content adheres to ethical guidelines, Legislation, Regulation and Codes of Practice.

Examples of Generative AI:

- Co-Pilot
- GPT-4
- ChatGPT
- Bard

b) **Automated Decision-Making Tools (ADMT).** Automated decision-making powered by AI holds great potential for optimising business operations, such as personalised recommendations, targeted advertising, and risk assessments. However, it is crucial to strike a balance between automation and human intervention, especially when dealing with sensitive matters like Subject Access Requests (SAR). Employees must ensure human oversight and accountability in AI-driven decisions to prevent biased outcomes and maintain compliance with data protection regulations.

Examples of ADMT:

- an online decision to award a loan
- a recruitment aptitude test which uses pre-programmed algorithms and criteria.

…

10 Publicity

10.1 YMCABCG acknowledges that at times, staff might come into contact with the media. All press enquiries should be directed through the Head of Communications or a member of staff to whom they escalate/delegate responsibility.

10.2 In the case of promotional materials, any images in which an individual is recognisable must only be used in instances in which a photo consent form has been obtained. In the case of any individual under the age of 18, this photo consent must be signed by an appropriate caregiver who has legal responsibility for the child (e.g. parent or guardian).

10.3 When YMCABCG carries out any direct communications as a way of marketing its services (such as events, fundraising exercises and soliciting donations) there will be a clear opt-out available.

10.4 When electronic mail addresses are collected any future use for marketing will be identified and a clear opt-in option made available.

11 Data Protection Issues Log

11.1 YMCABCG's Data Controller will maintain and keep up-to-date a Data Protection Issues Log which records significant activities and events and breaches in connection with the Association's implementation of Data Protection. By recording these, it will serve as evidence that appropriate efforts have been made to comply with **the Act** and serve as an annual evaluation aid.

11.2 All Data Protection Issues are to be reported in writing to the Data Controller in the first instance detailing the concern. Issues raised will be investigated within 7 working days with appropriate follow up action being taken which is to be documented on the Data Protection Issues Log.

11.3 YMCABCG is committed to protecting personal data / information. Following investigation of a Data Protection Issue, further action may be required which may include disciplinary action being taken. Failure to declare a Data Protection Issue in accordance with the Policy may result in disciplinary action.

11.4 YMCABCG will maintain an Access and Disclosure Log to monitor any access requests.

12 Data Retention Guide

12.1 YMCABCG provides a Data Retention Guide. A copy of the guide can be found at Appendix 1 and ensures minimum retention periods. Each project will agree on its retention periods that will be recorded by project managers.

12.2 Additionally, any stored items during the retention period will be securely stored in archive boxes that will include stored date, destruction date and contents guidance. A full inventory will be maintained on SharePoint by the Corporate Services Department.

13 Data Destruction

13.1 ***Day to Day Hard Copy Personal Data and Information***

On a day to day basis, hard copy data containing personal data is to be destroyed using a shredder provided by the organisation.

13.2 ***Archived Hard Copy Personal Data and Information***

It is the responsibility of projects to identify hard copy data which can be destroyed at the end of the Retention Period.

Hard copy data can only be destroyed using an approved external shredding company and a Certificate of Destruction must be provided to YMCABCG by them.

A schedule of the data destroyed must be attached to the Certificate and passed to YMCABCG's Data Protection Officer for retention.

13.3 ***Electronic Personal Data and Information***

The designated Responsible Persons for each project / site are responsible for the return of any unused or damaged devices and must ensure that unused items are stored securely within their setting.

YMCABCG Data Protection Officer has sole authority for the destruction of the Association's electronic devices.

Electronic devices (including mobile phones, tablets, laptops, desktop computers) are to be destroyed using approved WEEE compliant companies who must provide a Certificate of Destruction to YMCABCG.

A schedule of the devices and back-ups destroyed must be attached to the Certificate and retained by the Data Protection Officer.

14 Individual's Rights of Access

14.1 Individuals have several rights under **"The Act"**. These include the right to:

- Be Informed – to know what and how their data will be processed, for how long and where it may be shared. We do this through our privacy notices.
- Access – to request access to copies of personal data processed by a Controller (inclusive of that by a data processor).
- Rectification – to have inaccurate or incomplete data erased or rectified without undue delay.
- Erasure (right to be forgotten) – to ask for data to be deleted in circumstances where the data is no longer necessary, or consent is withdrawn without undue delay.
- Portability – Data provided by the data subject to the controller can be requested to be sent in a legible electronic format to another provider.
- Restriction of processing – the right to ask us to restrict the processing of personal information in certain circumstances.
- Object to automated decision making – Processing based solely on automated decision which produces legal effects to the individual.
- Object to processing – the right to object to the processing of personal information in certain circumstances, this can include marketing.

14.2 Anyone including an employee has these rights such as to request access to information kept about them by the organisation, including personnel files, sickness reports, disciplinary or training records, appraisal or performance review notes, emails in which the employee is the focus of the email and documents that are about the employee.

14.3 Individuals are not usually required to pay any charge for exercising these rights.

14.4 It is particularly important that if a person has made a Data Rights Request that this is forwarded to the HR Team. The association has only a calendar month in which to respond to a Subject Access Request free of charge. In some circumstances a fee may become applicable where allowable under "The Act". These are limited circumstances such as the request is regarded as manifestly unfounded, excessive or particularly if it is repetitive.

14.5 Certain data can be exempt from the right of access and other rights under "The Act" and this may include information which identifies other individuals, information that the association believes is likely to cause damage or distress, or information that is subject to legal professional privilege. Any exemptions will only be permissioned by the Chief Executive Officer in conjunction with the Data Protection Officer.

14.6 The association also treats as confidential any references given about one of its employees. The association recognises that an employee may have the right to access a reference received by the association. As such a reference will only be disclosed if such disclosure will not identify the source of the reference, and the referee has given their consent for disclosure, and the disclosure is reasonable in the circumstances.

14.7 The association may reserve its right to apply the appropriate statutory exemptions where they apply.

15 Redress

15.1 Any individual who considers that this policy has not been followed in respect of personal data about themselves should raise the matter with their line manager, the Data Protection Officer (DPO), or Executive Head of HR and Ethos if the individual involved with their line manager, using the Grievance Procedure

16 Review information

16.1 This policy and procedures will be reviewed every 2 years by the Chief Finance Officer and scrutinised by the Health and Safety Committee prior to being approved by the Board.

Further information regarding the Data Protection Act 2018 can be found at www.ico.gov.uk

Appendix 1 – UK GDPR Data Retention Quick Guide

The EU General Data Protection Regulation (GDPR), which came into force on 25 May 2018, brings in stricter requirements regarding how long personal data may be retained. Organisations will need to be more considered and disciplined in their retention of individuals' personal data. This quick guide is designed to help understand retention principles. Post Brexit, this is now referred to as the "UK GDPR."

What does the UK GDPR say about retaining personal data?

The emphasis under the GDPR is *data minimisation*, both in terms of the volume of data stored on individuals and how long it's retained.

To summarise the legal requirements, Article 5 (e) of the GDPR states personal data shall be kept for no longer than is necessary for the purposes for which it is being processed. There are some circumstances where personal data may be stored for longer periods (e.g. archiving purposes in the public interest, scientific or historical research purposes).

Recital 39 of the GDPR states that the period for which the personal data is stored should be limited to a strict minimum and that time limits should be established by the data controller for deletion of the records (referred to as erasure in the GDPR) or for a periodic review.

Organisations must therefore ensure personal data is securely disposed of when no longer needed. This will reduce the risk that it will become inaccurate, out of date or irrelevant.

Statutory Retention Periods

The table below summarises the main legislation regulating statutory retention periods. If employers are in doubt, it is a good idea to keep records for at least 6 years (5 in Scotland), to cover the time limit for bringing any civil legal action.

Record	Statutory Retention Period	Statutory Authority
Accident books, accident records/reports	3 years from the date of the last entry (or, if the accident involves a child/young adult, then until that person reaches the age of 21) (See below for accidents involving chemicals or asbestos)	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR) (SI 1995/3163) as amended, and Limitation Act 1980 Special rules apply concerning incidents involving hazardous substances (see below)
Accounting records	3 years for private companies, 6 years for public limited companies	Section 221 of the Companies Act 1985 as modified by the Companies Acts 1989 and 2006
Income tax and NI returns, income tax records and correspondence with HMRC	Not less than 3 years after the end of the financial year to which they relate	The Income Tax (Employments) Regulations 1993(SI 1993/744) as amended, for example by The Income Tax (Employments) (Amendment No.6) Regulations 1996 (SI 1996/2631)
Medical records and details of biological tests under the Control of Lead at Work Regulations	40 years from the date of the last entry	The Control of Lead at Work Regulations 1998 (SI 1998/543) as amended by the Control of Lead at Work Regulations 2002 (SI 2002/2676)
Medical records as specified by the Control of Substances	40 years from the date of the last entry	The Control of Substances Hazardous to Health Regulations

Hazardous to Health Regulations (COSHH)		1999 and 2002 (COSHH) (Sis 1999/437 and 2002/2677)
Medical records under the Control of Asbestos at Work Regulations. Medical records containing details of employees exposed to asbestos. Medical examination certificates	40 years from the date of the last entry, 4 years from the date of issue	The Control of Asbestos at Work Regulations 2002 (SI 2002/2675) Also see the Control of Asbestos Regulations 2006 (SI 2006/2739) and the Control of Asbestos Regulations 2012 (SI 2012/632)
Medical records under the Ionising Radiations Regulations 1999	Until the person reaches 75 years of age, but in any event for at least 50 years	The Ionising Radiations Regulations 1999 (SI 1999/3232)
Records of tests and examinations of control systems and protective equipment under the Control of Substances Hazardous to Health Regulations (COSHH)	5 years from the date on which the tests were carried out	The Control of Substances Hazardous to Health Regulations 1999 and 2002 (COSHH) (Sis 1999/437 and 2002/2677)
Records relating to children and young adults	Until the child/young adult reaches the age of 21	Limitation Act 1980
Retirement Benefits Schemes – records of notifiable events, for example, relating to incapacity	6 years from the end of the scheme year in which the event took place	The Retirement Benefits Schemes (Information Powers) Regulations 1995 (SI 1995/3103)
Statutory Maternity Pay records, Pay records, calculations, certificates (Mat B1s) or other medical evidence	3 years after the end of the tax year in which the maternity period ends	The Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960) as amended
Wage/salary records (also overtime, bonuses, expenses)	6 years	Taxes Management Act 1970
National minimum wage records	3 years after the end of the pay reference period following the one that the records cover	National Minimum Wage Act 1998
Records relating to working time	2 years from date on which they were made	The Working Time Regulations 1998 (SI 1998/1833)

Recommended (non-statutory) Retention Periods

For many types of personnel records, there is no definitive retention period: it is up to the employer to decide how long to keep these records. Different organisations make widely differing decisions regarding the retention periods to adopt. An employer needs to consider what would be a necessary retention period for them, depending on the type of record. The advice in this factsheet is based on the time limits for potential tribunal or civil claims, it is often a question of judgement rather than there being any definitive right and wrong.

Where the recommended retention period given is 6 years, this is based on the 6-year time limit within which legal proceedings must be commenced as laid down under the Limitation Act 1980. Thus, where documents may be relevant to a contractual claim, it is recommended that these be retained for at least the corresponding 6-year limitation period.

Record	Recommended Retention Period
Actuarial valuation reports	Permanently
Application forms and interview notes (for unsuccessful candidates)	6 months to a year (because of the time limits in the various discrimination Acts, minimum retention periods for records relating to advertising of vacancies and job applications should be at least 6 months. A year may be more advisable as the time limits for bringing claims can be extended. Successful job applicants documents will be transferred to the personnel file in any event.
Assessments under health and safety regulations and records of consultations with safety representatives and committees	Permanently
Inland Revenue/HMRC approvals	Permanently
Money purchase details	6 years after transfer or value taken
Parental leave	5 years from birth/adoption of the child or 18 years if the child receives a disability allowance.
Pension scheme investment policies	12 years from the ending of any benefit payable under the policy
Pensioners' records	12 years after benefit ceases
Personnel files and training records (including disciplinary records and working time records)	6 years after employment ceases
Redundancy details, calculations of payments, refunds, notification to the Secretary of State	6 years from the date of redundancy
Senior executives' records (that it, those on a senior management team or their equivalents)	Permanently for historical purposes
Statutory Sick Pay records, calculations, certificates, self-certificates	The Statutory Sick Pay (Maintenance of Records) (Revocation) Regulations 2014 (SI 2014/55) abolished the former obligation on employers to keep these records. Although there is no longer a specific statutory retention period, employers still have to keep sickness records to best suit their business needs. It is advisable to keep records for at least 3 months after the end of the period of sick leave in case of a disability discrimination claim. However, if there were to be a contractual claim for breach of an employment contract it may be safer to keep records for 6 years after the employment ceases.
Time cards	2 years after audit
Trade union agreements	10 years after ceasing to be effective
Trust deeds and rules	Permanently
Trustees' minute books	Permanently
Works council minutes	Permanently

Appendix 2 - Summary of Amendments V3 to V4

- Section 1.1: Last sentence changed to read "There are safeguards within the Data Protection Act 2018"

- Section 1.2: First sentence updated to read, "which came into force on 25th May 2018"

- Section 1.2: The following additional laws were added to this section:
- UK General Data Protection Regulation (UK GDPR)
- Privacy and Electronic Communications Regulations (PECR)
- Digital Economy Act (DEA)
- Environmental Information Regulations 2004

- Section 3.2: Changed from Chief Corporate Officer to Chief Finance Officer.
- Section 6.2: last bullet point changed to 12 from (10) for Data destruction.

- Section 6.3: Updated to read "Staff will utilise Multi Factor Authentication (MFA) to access corporate systems including E-Mail."
- Section 7.2: changed to read "between 14 and 28 days depending upon the DVR's capacity".
- Section 8.3: Updated as RDWeb is no longer used.

- Section 9.1: Changed Communications and Community Relations Officer to Head of Communications.

- Section 12.1 Updated to state that shredding bags are no longer used and copies of personal data and information should be destroyed using a shredder provided by the organisation.

- Section 15.1: Changed from Chief Corporate Officer to Chief Finance Officer.

Appendix 3 – Summary of Amendments v4 to V5

Section 1

- Added 1.1. This addition has been recommended to ensure the designation of data controller aligns with the legislation and the structure of the organisation as the organisation processes personal data as a data controller and data processor.
- Updated what was section 1.1, now 1.2 to explain why the data protection policy exists
- 1.3 updated and expanded to include compliance with codes of practice. E.g. the ICO's Statutory Data Sharing Code of Practice and the CCTV Code of Practice.
- 1.6 now includes our ICO registration number
- 1.7 provides additional clarity on who the policy applies
- 1.8 provides additional clarity on aligned policies and confirms how it aligns to HR processes.

Section 2

- Under 2.2g amended to terminology to align with the 7th Principle of the UK GDPR, that of Accountability.
- Added 2.3 to define the term "processing"
- Added 2.4 provides additional clarity on the lawful bases for processing personal data.

Section 3

- Updated the Roles and Responsibilities table to reflect the appropriate roles & tasks. The Data Controller now refers to the Organisation rather than an individual, the DPO

tasks have been aligned with the tasks of the DPO as outlined in the UK GDPR, and confirmed the HR team are responsible for overseeing all Data Rights requests, not just Subject Access Requests.

Section 4
- Added 4.5 to explain the sources of where we may collect personal data from
- Added 4.6 to state the privacy notice provides further details

Section 5
- Fixed small typo in 5.2

Section 6
- 6.1 Updated to reflect that UK are no longer in the EU
- 6.2 Updated to provide clarity and around the responsibility of all parties who handle personal data, and that this is not just limited to staff and volunteers.
- 6.4 Updated to ensure the clause applies to all teams, not just volunteers

Section 7
- 7.3 Amended to state the privacy notice provides further details
- 7.4 Amended to state that we will also comply with the requirements laid out by Biometrics and Surveillance Camera Commissioner and the Surveillance Camera Code of Practice.

Section 8
- 8.2 has been expanded to make it clear that where personal devices are used, there must also be no access to organisational data by any other users of the devices.
- 8.4 expanded to be clear that devices must not be left unattended at any time included working remotely.
- 8.5 amended to be clear that the responsibility sits with the device user/owner as the terms staff and volunteer felt to generalised.

Section 9
Added full new section on the use of Artificial Intelligence to ensure it is clear on what our approach is
Section 14 (was 13)
- 14.1 has been amended to ensure it is clearly documented that the right of access is not absolute and that that data subjects do not have the right to "see" all data, but they have the right to ask for copies of their personal data, and that there are exemptions that will limit what can be disclosed.
- Updated the definition of "Restriction of processing"
- Updated the definition from Object to Marketing and changed to "Object to Processing" as documented in the UK GDPR as the right is wider than just to object to marketing.
- Added 14.3 to be clear that individuals are not usually required to pay.
- 14.4 and 14.5 have been amended to ensure it encompasses all rights and not just Subject Access Requests.
- 14.5 now also includes the requirement to engage the DPO in this process
- 14.7 has been amended to provide clarity around how and why the organisation applies exemptions as the current wording could have been misinterpreted.

Section 15
- 15.1 now also includes the requirement to engage the DPO in this process