DATA PROTECTION POLICY

Policy Type:	BOARD
Policy Area:	Corporate
Policy Number:	8c V3
Produced by:	Chief Corporate Officer
Issued to SLT for input:	23 November 2021 for input by 3 December 2021
Scrutinised by the Health and Safety Committee:	Minor amendments only made to the Policy as set out at Appendix 2
Approved by the Board:	2 February 2022
Issued Date	To all staff for signing via People HR
Review Date:	February 2024

CONTENTS

1 Introduction

1.1 In order to operate efficiently, YMCA Black Country Group ("YMCABCG") 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, 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. There are safeguards within the Data Protection Act 1998 to ensure this.

1.2 YMCABCG is fully committed to comply with the requirements of the Data Protection Act 2018 ("**the Act**"), which came into force on 1st March 2000. This policy has been prepared in accordance with its requirements, along with the following legislation and regulations:

- 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

1.3 **The Act** gives protection to individuals about whom 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.

1.4 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**.

1.5 In addition, YMCABCG will register, where appropriate, with the Information Commissioner's Office.

1.6 This Policy applies to all YMCA Black Country Group members including its subsidiaries and associated companies.

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

- Disciplinary Procedures;
- Staff Handbook; and
- Whistleblowing Policy.

2 Scope

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

2.2 YMCABCG will comply with the eight data protection principles per the Data Protection Act:

- Personal data shall be collected fairly and lawfully
- Personal data shall only be obtained for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose/those purposes.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose for which they are being processed.
- Personal data shall be adequate and, where necessary, kept up-to-date.
- Personal data processed for any purpose shall not be kept for longer than necessary for that purpose.
- Personal data shall be processed in accordance with the rights of the data subjects under the Act
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of or damage to personal data.
- Personal data shall not be transferred to a country or territory outside of the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of their data.

3 Handling of Personal/Sensitive Data

3.1 **The Act** provides conditions for the processing of personal data. It also makes a clear distinction between **personal data and "sensitive" personal data.**

Personal data is defined as data relating to a living individual who can be identified from either (a) the data or (b) that data and other information that is in the possession of, or likely to come into the possession of, the data controller and includes an expression of opinion about the individual and any indication of the intention of the data controller or any other person in respect of the individual.

Sensitive personal data is defined as personal data consisting of information as to: racial or ethnic origin; political opinion; religious or other beliefs; trade union membership; a physical or mental health condition; sexual life; and/or criminal proceedings/convictions.

Data Controller is the Chief Corporate Officer. YMCABCG reserves the right to transfer this role to another member of staff if seen appropriate by the CEO/Executive Management.

Data Protection Officer is the Health, Safety and Environmental Manager and has overall responsibility for the provision of data protection training for staff and volunteers within the association, the development of best practice guidelines, the maintenance of aforementioned Issues Log, and to ensure adherence through regular evaluation. YMCABCG reserves the right to delegate this role to another member of staff if seen appropriate by the Chief Officer / Executive Management / Senior Leadership Team.

3.2 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 EEA without suitable safeguards.
- Ensure the rights of people about whom the information is held can be fully exercised under **the Act**.

3.3 In addition, YMCABCG will ensure:

- There is a specific named person within the Association with responsibility for data protection.
- All staff and volunteers who handle personal information are aware of their personal responsibilities and wider organisational responsibilities for following good data protection practice.
- All staff and volunteers handling personal information is appropriately trained to do so.
- All staff and volunteers managing and handling personal information is appropriately supervised.
- Staff and volunteers 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 10 "Data Destruction"

3.4 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 (see section 6.1)

3.5 It is the responsibility of the appropriate manager to ensure that their team's volunteer(s) is made fully aware of this policy and their duties and responsibilities.

3.6 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.

4 CCTV

4.1 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.

4.2 In terms of CCTV, YMCABCG images are kept for a rolling 28 day period. 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.

4.3 Where CCTV is in operation, signs will be displayed.

4.4 YMCABCG ensures the safe handling of CCTV images in accordance with the handling of personal data outlined under **the Act**.

5 Computer Use, Electronic Communications and Wireless Internet Connections

5.1 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.**

5.2 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.

5.3 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 5.1 above is used. When using public networks you must only access the Association's email system, files or databases using Outlook Web Access for emails and SharePoint sites or RDWeb (for remote Web Apps and computer access) for files and databases:

Outlook Web Access: https://mail.ymcabc.org.uk/owa

RDWeb - Either: https://wbremote.ymcabc.org.uk/RDWeb or https://wremote.ymcabc.org.uk/RDWeb

All of the above connections are secure and encrypted.

Copies of the Guides for both Outlook Web Access and RDWeb can be found within the IT Policies and Procedures section on SharePoint.

5.4 Under no circumstances must you leave either a device supplied by the Association or a personal device unattended whilst using public networks.

5.5 It is the responsibility of staff and volunteers 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.

5.6 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 EEA

5.7 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.

6 Staff Individual Responsibilities

6.1 All staff have a duty to protect personal data/personal information. Therefore:

- Staff will not disclose personal data to anybody internal or external to the organisation who doesn't need to know.
- Staff will not leave the desktop of their PC/laptop/mobile device unlocked when unattended.
- Staff will change their passwords when prompted to do so and keep these passwords secure from internal colleagues and external sources.
- Staff will not allow unauthorised persons to view screen
- Staff will not leave computer print outs containing personal data/information in the printer, on their desk or in an unlocked drawer
- Staff will not use data for a purpose other than that stated on service user registration.
- Staff will keep all files, documents and information containing personal data, paper or electronic, secure.
- Staff will not 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.
- Staff will not make subjective statements/statements of opinion on service user records.

7 Publicity

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

7.2 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 care-giver who has legal responsibility for the child (e.g. parent or guardian).

7.3 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.

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

8 Data Protection Issues Log

8.1 YMCABCG 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.

8.2 All Data Protection Issues are to be reported in writing to the Chief Corporate Officer 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.

8.3 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.

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

9 Data Retention Guide

9.1 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.

9.2 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.

10 Data Destruction

10.1 ***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.

Alternatively, hard copy data can be stored securely and locked away before being transferred to a shredding bag, secured by cable tie and stored in a safe, secure and non-hazardous location to be shredded periodically. Shredding bags and cable ties are available, on request, from the Data Protection Officer.

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

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

10.2 ***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.

10.3 ***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.

11 Access to Information

11.1 Any person about whom YMCABCG holds personal data (staff, volunteers, service users, partners, donors) has the right, under law, to request a copy of that information. If requested, the Association will:

- Respond to the request in a reasonable amount of time (no more than 40 days)
- Make a discretionary administration charge of £10 on each occasion that access is requested.

12 Redress

12.1 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, or Executive Head of HR and Ethos if the individual involved with their line manager, using the Grievance Procedure.

13 Review information

13.1 This policy and procedures will be reviewed every 2 years by the Chief Corporate 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	40 years from the date of the last entry	The Control of Lead at Work Regulations 1998 (SI 1998/543)

tests under the Control of Lead at Work Regulations		as amended by the Control of Lead at Work Regulations 2002 (SI 2002/2676)
Medical records as specified by the Control of Substances Hazardous to Health Regulations (COSHH)	40 years from the date of the last entry	The Control of Substances Hazardous to Health Regulations 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 V2 to V3

1. **Amended** – 9.1 to make reference to Appendix 1
2. **Amended –** 13.1 to refer to scrutiny of Policy by the Health and Safety Committee prior to being approved by the Board.
3. **Added for ease of reference** – Appendix 1 – UK GDPR Data Retention Quick Guide