Data Protection Policy

Contents

Change History

Version number	Date of Release	Policy Owner	Authorised by
1.0	08/11/16	Aimee Henderson, Group Finance Director & Company Secretary (SIRO)	Audit & Risk Committee
2.0	22/02/18	Aimee Henderson, Group Finance Director & Company Secretary (SIRO)	Board of Trustees
3.0	30/05/18	Aimee Henderson, Group Finance Director & Company Secretary (SIRO)	Board of Trustees
4.0	30/07/20	Ryan Palmer, Director of Quality & Impact (SIRO)	Board of Trustees

Policy Statement

- Central YMCA ('the Charity') fully understands its obligations to ensure that personal information is treated fairly, lawfully and correctly, and it is committed to achieving compliance with relevant Data Protection legislation.
- The Charity needs to collect and process personal data about people, including staff and individuals with whom it deals with, to operate its daily business and for the organisation to operate effectively.
- The Data Protection Act 2018 ('the Act') and the General Data Protection Regulation (2016/679) ('GDPR') sets out the rules about how personal data and sensitive personal data about living individuals must be processed.
- Most businesses hold personal data on their customers, employees and partners. The explosion in the use of the Internet, electronic communication and computerisation of business data has led to an increase in the importance of privacy. Breaches of computerised data security have prompted the introduction of legislation on a national and European level. These include:

    - Human Rights Act 1998;
    - Freedom of Information Act 2000;
    - Privacy and Electronic Communications Regulations 2003;
    - Regulation of Investigatory Powers Act 2000;
    - Telecommunications (Lawful Business Practice) Interception of Communications Regulations 2000;
    - The Act;
    - Computer Misuse Act 1990; and
    - GDPR.

- The GDPR replaces the Data Protection Directive (Directive 95/46/EC) ('the Directive') and supersedes the laws of individual Member States that were developed in compliance with the Directive. Its purpose is to protect the "rights and freedoms" of living individuals, and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.
- The Charity aims to ensure that information held about employees, ex-employees, volunteers and service users is relevant and accurate; stored safely and available to individuals within reasonable timescales.
- The Charity is committed to ensuring that staff are appropriately trained and supported to achieve compliance with the Data Protection Act and other relevant legislation. This is regarded by the Charity as vital in maintaining the confidence between Central YMCA and with those whose personal data they hold.
- The Charity fully endorses and adheres to the Data Protection Principles listed below:
    - personal data shall be processed fairly and lawfully;
    - personal data shall be obtained only for specified and lawful purposes, and shall not be processed in any manner incompatible with those purposes;
    - personal data shall be adequate, relevant and not excessive in relation to the purposes for which it is processed;
    - personal data shall be accurate and, where necessary, kept up to date;
    - personal data shall be kept for no longer than is necessary for the purposes for which it is processed;
    - personal data shall be processed in accordance with the rights of Data Subjects under the Bill and GDPR (General Data Protection Regulations);
    - personal data shall be subject to appropriate technical and organisational measures to protect against unauthorised or unlawful processing and accidental loss, destruction or damage;

- personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of data protection.

- Trustees and the Executive Team are strongly committed to the rights of individuals (the 'Data Subjects') whose data they collect and process and will comply with UK and EU laws related to personal information in line with the GDPR. These include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.
- This policy describes how this personal data must be collected, handled and sorted to meet the company's data protection standards and to comply with the law.

Scope

- This policy applies to all personal data and sensitive personal data collected and processed by the Charity in the conduct of its business, in electronic medium and within structured filing systems.
- This policy applies to all Charity employees ('all staff'), whether permanent, temporary, contractors, consultants or volunteers.
- The Central Young Men's Christian Association (Central YMCA) is the data controller and is registered with the Information Commissioner's Office ('ICO') for collecting and using personal data to:
- provide education and training to our students, customers and clients as well as administer membership records for the Charity. Personal information is also processed to enable us to provide a voluntary service for the benefit of the public; to fundraise and promote the interests of the charity; manage our employees and This data protection policy ensures that Central YMCA:
    - complies with data protection law and follows good practice;
    - protects the rights of staff, customers and partners;
    - is open about how it stores and processes individuals' data; and
    - protects itself from the risks of a data breach.

Related Policies, Procedures, and Templates

- Records Retention & Disposal Policy
- Record Retention Schedules
- Privacy Notice

Responsibilities

Individual Responsibilities

Board of Trustees	Overall responsibility for the policies and procedures that govern the work at Central YMCA.
Chief Executive	Overall responsibility for ensuring Central YMCA's resources are used effectively and appropriately.
Senior Information Risk Officer (SIRO)	Responsible for understanding how the strategic business goals of the organisation may be impacted by any information risks, and for taking steps to mitigate them. The SIRO is accountable and responsible for information risk across the Charity.
Data Protection Officer (DPO)	Accountable to the SIRO and responsible for the management of personal information within Central YMCA and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes the development and implementation of the data protection policy and security and risk management to ensure compliance.
Policy Owner	Responsible for ensuring guidelines are in place and that policies and procedures reflect our charitable ethos and commitment to equality and diversity.
All Line Managers	Responsible for ensuring all employees are aware of and follow this policy.
All Employees and Volunteers	To follow policies and procedures, promoting best practice throughout the organisation.

- Everyone who works for or with Central YMCA has the responsibility for ensuring data is collected, stored and handled appropriately.
- Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.
- All third parties who require access to personal data will be required to sign a confidentiality agreement before access is permitted. This agreement will ensure that the third party has the same legal obligations as the Charity. This will also include an agreement that the Charity can audit compliance with the agreement.
- Any breach of the GDPR or this policy, will be considered as a breach of the disciplinary policy and could also be considered a criminal offence, potentially resulting in prosecution.

Company Responsibilities

- Central YMCA is both a data controller and data processor as defined under the GDPR.
- Senior Management and all those in managerial or supervisory roles throughout Central YMCA are responsible for developing and encouraging good information handling practices within the organisation; responsibilities are set out in individual job descriptions.
- Central YMCA has appointed a suitably qualified and experienced DPO who is responsible for day to day compliance with this policy. The DPO is responsible for ensuring that Central YMCA complies with the GDPR in relation to all aspects of data processing. The DPO has direct responsibility for policy and procedures, including Subject Access Requests. The DPO is also the person to whom all staff should seek guidance regarding GDPR compliance.
- It should be noted that compliance with GDPR requirements remains the responsibility of all staff who process or control personal information for Central YMCA. All members of staff employed by the Charity are also responsible for ensuring that any personal data that is about them that is supplied by them to the Charity is accurate and up-to-date.

The Charity is responsible for ensuring that staff have regular suitable training in order to undertake their data protection responsibilities.

Policy Review

Review of impact against the aims of policy:

This policy has been reviewed by Ryan Palmer (SIRO) and Lucian-Gabriel Burcea (DPO). They have been approved by the Board of Trustees and are deemed fit for purpose. All related procedures have been designed to match the contents of this policy.

The policy has been communicated successfully to all employees and has been made available on the Charity's intranet.

Does there appear to be any patterns of equality related issues: No

If yes, please provide an Equalities Impact Assessment (if relevant): N/A

Reviewed by: **Date:**

This policy will be reviewed on an annual basis by the Policy Owner and signed off by the Board of Trustees if any changes are made.

Next review date: July 2020

Policy

The objectives of this policy are to ensure that:

- Proper procedures are in place for the processing and management of personal data;
- There is documentation within the organisation to provide knowledge about data protection compliance;
- All staff understand their responsibilities when processing personal data, and that methods of handling that information are clearly understood;
- Individuals are assured that their personal data is processed in accordance with the data protection principles, that their data is secure and safe from unauthorised access, alteration, use or loss;
- Other organisations with whom the Charity needs to share or transfer data, meet compliance requirements;
- Any new systems being implemented are assessed on whether they will hold personal data, whether the system presents any risks, damage or impact to individuals' data and that it meets this policy.

1. Fair Collection and Processing

- The specific conditions contained in the Data Protection Act regarding the fair collection and use of personal data will be fully complied with.
- Individuals will be made aware that their information has been collected, and the intended use of the data specified either on collection or at the earliest opportunity following collection.
- Personal data will be collected and processed only to the extent that it is needed to fulfil business needs or legal requirements.
- Personal data held will be kept up to date and accurate.
- Retention of personal data will be appraised, and risk assessed to determine and meet business needs and legal requirements, with the appropriate retention schedules and disposal of applied to that data.

- Personal data will be processed in accordance with the rights of the individuals about whom the personal data are held.
- Further guidelines around the storage and management of data can be found in Appendix F

2. Security

- Appropriate technical, organisational and administrative security measures to safeguard personal data will be in place.
- Staff are required to report any actual, near miss, or suspected data breaches to the SIRO (Senior Information Risk Owner) for investigation. Lessons learnt during the investigation of breaches will be relayed to those processing information to enable necessary improvements to be made.
- An Information Asset Register will be maintained identifying personal data held, where it is held, how it is processed and who has access to it.
- Appropriate technical, organisational and administrative security measures to safeguard personal data will be in place.
- Data Protection Awareness Training will be provided, as appropriate, to staff to keep them better informed of relevant legislation and guidance regarding the processing of personal information.
- Both the GDPR and the Data Protection Act require that personal data is securely handled, therefore, it is considered an employment offence to save personal data on local drives or computer desktops without authorisation. Removal of confidential or personal data offsite is discouraged, however, under certain circumstances personal data may be downloaded onto local drives or computer desktops if authorisation from the Department Manager has been gained before doing so. Staff should make requests in writing stating why downloading or transportation of data is required, physical address of storage location, and identify any risks associated with transportation and offsite storage.
- Further guidelines around data security can be found in Appendix F

3. Data Protection Impact Assessments

- All teams will work with the Data Protection Officer to carry out Data Protection Impact Assessments on all new systems intended for implementation by the Charity, with the intent to determine the risks and impacts to personal data of the individuals those systems are intended to hold.

4. Data Sharing

- Personal data will not be transferred outside the European Economic Area (EEA) by the Charity, unless that country or territory can ensure a suitable level of protection for the rights and freedoms of the Data Subjects in relation to the processing of their personal data.
- Personal data in any format will not be shared with a third-party organisation without a valid business reason, a signed Data Sharing Agreement in place, or without the Data Subjects' consent.
- Further guidelines regarding the transfer of data outside the EEA can be found in Appendix E

5. Access and Subject Access Requests

- Members of staff will have access to personal data only where it is required as part of their functional remit.
- All individuals who are the subject of personal data held by the Charity are entitled to:
  - Ask what information the company holds about them and why;
  - Ask how to gain access to it;

- Be informed how to keep it up to date; and
- Be informed how the company is meeting its data protection obligations.

- If an individual contacts the company requesting this information, this is called a Subject Access Request. Subject Access Requests from individuals should be made by any digital means or addressed to the Charity. Subject Access Requests are free of charge, unless there are excessive requests coming from a certain individual.
- The Charity's Privacy Notice will include a contact address for Data Subjects to use should they wish to submit a Subject Access Request, make a comment or complaint about how the Charity is processing their data, or about the Charity's handling of their request for information.
- Subject Access Requests will be acknowledged to the Data Subject within 3 working days, with the final response and disclosure of information (subject to exemptions) within 30 days from verification. In certain circumstance we may request an extension of two more months. The Charity must always verify the identity of anyone making a subject access request before handing over any information and should seek guidance from the Data Protection Officer.
- In certain circumstances, the Act allows personal data to be disclosed to law enforcement agencies without the consent of the Data Subject. Only under such circumstances, the Charity will disclose requested data. However, the Data Protection Officer will ensure the request is legitimate, seeking assistance from the Charity's legal advisers where necessary

6. Data Breaches

- A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.
- All employees must report a breach, or suspected data breach to their manager and the Data Protection officer.
- When a personal data breach has occurred, the Data Protection Officer will assess the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then the Charity must notify the Information Commissioner's Office (ICO); if it's unlikely then it is not necessary to report it, however such decisions must be justified and documented. A notifiable breach to the ICO must be made without undue delay, but not later than 72 hours after becoming aware of it.

7. Consent

- The Charity understands 'consent' to mean that it has been explicitly and freely given, specific, informed and an unambiguous indication of the Data Subject's wishes by which he or she by statement, or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The consent of the Data Subject can be withdrawn at any time.
- In addition, the Charity understands 'consent' to mean that the Data Subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or based on misleading information will not be a valid basis for processing. There must be some active communication between the parties which demonstrate active consent. Consent cannot be inferred from non-response to a communication. For sensitive data, explicit written consent of Data Subjects must be obtained unless an alternative lawful basis for processing exists.

- Consent to process personal and sensitive data is obtained routinely by the Charity using standard consent documents. This may be through a contract of employment or during induction.
- Where the Charity provides online services to children, parental, or custodial authorisation must be obtained. This requirement applies to children under the age of 16 (unless the Member State has made provision for a lower age limit – which may be no lower than 13.

8. Complaints

- A Data Subject has the right to complain to the Charity at any time if they have concerns about how their information is used.
- A Data Subject also has the option to complain directly to the Information Commissioners Office. Details of the options for lodging a complaint is provided within Privacy Notice available on the Charity's website.

Appendix A: Data Controller Names for the Central YMCA Group

Data Controller: The Central Young Men's Christian Association. **Registration Number:** Z670975X

Address:
112 Great Russell Street
London
WC1B 3BQ

Other Names:
CENTRAL SERVICES
CENTRAL YMCA
ONE KX
POSITIVE HEALTH
THE CLUB
YMCA AWARDS
YMCA FITNESS INDUSTRY TRAINING (YMCAFIT)
YMCA TRAINING

Appendix B: Data Protection Definition and Terms

Data	Information which is recorded in any format, whether stored electronically or in a structured paper-based filing system.
Personal Data	Any information that identifies a living individual. This includes any expression of opinion about the individual and any Intentions towards the individual.
Sensitive Personal Data	Personal information relating to racial or ethnic origin, political opinion, religious beliefs, trade union membership, sexual life, physical or mental health, commission or alleged commission of any offence.
Processing	Any activity where the data is used, such as obtaining, recording, storing, viewing, copying, accessing, disclosing, erasing, destroying.
Data Subject	An individual who is the subject of personal information.
Data Controller	The organisation that determines how the personal data will be used and the way it will be processed.
Data Processor	An organisation that processes personal data on behalf of a Data Controller.
Subject Access Request	A request by a Data Subject, to the data controller, asking to see their personal information.
Third Party	This can either mean that the data is about someone else, or someone else is the source; i.e. any other person or organisation other than -the Data Subject; -the data controller; -a data processor.

Appendix C: Conditions for Processing Personal Data

The Data Protection Bill requires personal data to be processed fairly and lawfully, and, not to be processed unless one of the conditions (below) is met.

At least one of the following conditions must be met for personal information to be considered fairly processed:

- the individual has consented to the processing
- processing is necessary for the performance of a contract with the individual
- processing is required under a legal obligation (other than one imposed by the contract)
- processing is necessary to protect the vital interests of the individual
- processing is necessary to carry out public functions, e.g. administration of justice
- processing is necessary to pursue the legitimate interests of the data controller or third parties

Appendix D: Rights under the Act

There are eight rights under the Data Protection Bill:

1. **The right to be informed**
   The right to be informed covers some of the key transparency requirements of the GDPR. It is about providing individuals with clear and concise information about what we do with their personal data.

2. **The right of Access**
   The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data as well as other supplementary information. It helps individuals to understand how and why we are using their data, and check we are doing it lawfully.

3. **The right to rectification**
   Individuals have the right to have inaccurate personal data rectified. An individual may also be able to have incomplete personal data completed – although this will depend on the purposes for the processing. This may involve providing a supplementary statement to the incomplete data.

4. **The right to erasure**
   Individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances.

5. **The right to restrict processing**
   An individual has the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way that an organisation uses their data. This is an alternative to requesting the erasure of their data.

6. **The right to data portability**
   The right to data portability gives individuals the right to receive personal data they have provided to a controller in a structured, commonly used and machine-readable format. It also gives them the right to request that a controller transmits this data directly to another controller.

7. **The right to object**
   Individuals have the right to object to the processing of their personal data. This effectively allows individuals to ask us to stop processing their personal data. The right to object only applies in certain circumstances. Whether it applies depends on our purposes for processing and our lawful basis for processing.

8. **Rights in relation to automated decision making and profiling**
   Individuals who are Data Subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

Appendix E: Privacy Electronic Communication Regulations 2003

- The Privacy and Electronic Communications (EC Directive) Regulations 2003 ('PECR') are derived from European law. They implement European Directive 2002/58/EC, also known as 'the e-privacy Directive'.
- The e-privacy Directive complements the general data protection regime and sets out more-specific privacy rights on electronic communications. It recognises that widespread public access to digital mobile networks and the internet opens up new possibilities for businesses and users, but also new risks to their privacy.
- PECR have been amended seven times. The more recent changes were made in 2018, to ban cold-calling of claims management services and to introduce director liability for serious breaches of the marketing rules; and in 2019 to ban cold-calling of pension schemes in certain circumstances.
- This guide covers the latest version of PECR, which came into effect on 9 January 2019, with some updates to cover changes made by the GDPR from 25 May 2018.
- The EU is in the process of replacing the e-privacy Directive with a new e-privacy Regulation to sit alongside the GDPR. However, the new Regulation is not yet agreed. For now, PECR continues to apply alongside the GDPR.
- Personal data shall not be transferred to a country or territory outside the European Union Member States 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 personal data.
- The transfer of personal data outside of the EU Member States is prohibited unless one or more of the safeguards or exceptions specified below apply:

Binding corporate rules	Central YMCA may adopt approved Binding Corporate Rules for the transfer of data outside the EU Member States.
Model contract clauses	Central YMCA may adopt approved model contract clauses for the transfer of data outside of the EU Member States. If Central YMCA adopts the model contract clauses approved the relevant Supervisory Authority, there is an automatic recognition of adequacy.
Ad Hoc contractual clauses	Central YMCA may adopt ad hoc contractual clauses that will have to be approved by the ICO. They allow the Central YMCA to individually tailor the transfer to its needs, however, the provisions for such clauses may differ at the member state level.
Exceptions	In the absence of the above, transfer of data shall only take place subject to the fulfilment of the following conditions: • the Data Subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the Data Subject due to the absence of an adequacy decision and appropriate safeguards; • the transfer is necessary for the performance of a contract between the Data Subject and the controller or the implementation of pre-contractual measures taken at the Data Subject's request; • the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the controller and another natural or legal person; • the transfer is necessary for important reasons of public interest; • the transfer is necessary for the establishment, exercise or defence of legal claims;

	• the transfer is necessary to protect the vital interests of the Data Subject or of other persons, where the Data Subject is physically or legally incapable of giving consent; • the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case.

- The Charity's Data Protection Officer will assess the adequacy of the safeguards considering the following factors:
  - the nature of the information being transferred;
  - the country or territory of the origin, and destination, of the information;
  - how the information will be used and for how long;
  - the laws and practices of the country of the transferee, including relevant codes of practice and international obligations; and
  - the security measures that are to be taken about the data in the overseas location. (This is a UK-specific option.)

A list of countries that satisfy the adequacy requirements of the Commission are published in the Official Journal of the European Union and in the GDPR.

Appendix F: Data Storage and Management

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT Manager or Data Protection Officer.

Hard Copies

- When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.
- These guidelines also apply to data that is usually stored electronically but has been printed out for some reason. In such instances:
  - When not required, the paper or files should be kept in a locked drawer or filing cabinet;
  - Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer;
  - Data printouts should be shredded and disposed of securely when no longer required.

Soft Copies

- When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts
- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a USB, CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.

- Data should be backed up frequently. Those backups should be tested regularly, in line with the Charity's standard back up procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.

Data use

- Personal data is of no value to the Charity unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft.
- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended
- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure
- Data must be encrypted before being transferred electronically
- Personal data should never be transferred outside of the European Economic Area
- Employees should not save copes of personal data to their own computers. Always access and update the central copy of any data.

Data accuracy

- The law requires the Charity to take reasonable steps to ensure data is kept accurate and up to date.
- The more important it is that the personal data is accurate, the greater the effort the Charity should put into ensuring its accuracy.
- It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date possible.
- Data will be held in as few places as necessary and should not be duplicated wherever possible
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- Central YMCA will make it easy for Data Subjects to update the information the Charity holds about them. Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the marketing department's responsibility to ensure marketing databases are checked against industry suppression files every six months.