Created by: Georgina Jones, Director of Resource and Risk Management May 2018
Approved by: Martin Hodgson, Chief Executive on 2018
Review date: May 2021

GENERAL DATA PROTECTION REGULATION
Policy and Procedure
Effective from 25th May 2018

YMCA Somerset Coast's work involves confidential information and confidentiality must be respected at all times. Communication is imperative to the work of the Association. However, checks and measures are necessary to avoid the betrayal of a confidence and the Association's staff, volunteers and trustees must adhere to the guidelines below. The collection and retention of data and the unauthorised disclosure to another party of information deemed to be confidential and gained in the course of work within the Association will be treated as gross misconduct within the terms of our disciplinary procedure.

The aim of the General Data Protection Regulation Policy & Procedure is to ensure that all staff and volunteers are aware of their responsibilities and obligations in relation to personal information held.

1. Responsibility

1.1 The Board of Directors, in association with the Chief Executive, has overall responsibility for ensuring this policy complies with our legal and ethical obligations, and that all those under our control comply with it.

1.2 The Chief Executive and the Director of Resource and Risk Management have day-to-day responsibility for implementing this Policy and procedure, and for monitoring its use and effectiveness.

1.3 It is the responsibility of line managers to communicate the requirements of this policy and procedure to their employees, and to ensure adherence.

2. Purpose of Policy

2.1 The purpose of this policy and procedure is to ensure that staff understand and comply with the requirements of the General Data Protection Regulation, ad explains the requirements for collection, storing, processing and deleting data in addition to the expectations of all employees. This policy will be in effect from 25th May 2018.

2.2 The policy will outline the requirements of the General Data Protection Regulation.

2.3 The policy will highlight the importance of compliance and explain the expectations of all staff.

2.4 The policy will outline the responsibilities of each individual.

2.5 The policy will reduce risk and foster a culture of best practice.

2.6 The policy will ensure the security of the personal data held by the organisation.

.

3. Scope

3.1 This policy applies to all YMCA Somerset Coast staff working in all properties owned and/or managed by YMCA Somerset Coast. Contractors, staff members and out-of-hours operators are expected to comply with it.

4. Expectations and Policy Compliance of the Organisation

4.1 As an employee, we expect you to:

4.1.1 Behave honestly, responsibly and within the guidelines of this policy.
4.1.2 Understand the definitions explained under the policy and the principles of General Data Protection Regulation.
4.1.3 Prioritise confidentiality of personal data and escalate queries as necessary.

4.2 As a manager, we expect you to:

4.2.1 Behave honestly, responsibly and within the guidelines of this policy.
4.2.2 Understand the definitions explained under the policy and the principles of General Data Protection Regulation.
4.2.3 Ensure that staff teams have a good understanding of the requirements of the policy and provide training where needed.
4.2.4 Prioritise confidentiality and escalate queries as necessary.

4.3 If employees do not comply with the policy we may review processes and responsibilities in the role. Persistent or deliberate non-compliance may result in disciplinary action and could be deemed to be gross misconduct.

5. Overview of Data

5.1 Personal data is defined in Article 4 of the General Provisions of General Data Protection Regulation as:

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

5.2 It will be necessary to collect, process and store personal data as part of many of the daily activities carried out by the organisation.

5.3 Data that is more sensitive and therefore needs more protection is termed as Special Category data under GDPR. This type of data could create more risk to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination.

5.4 Examples of special category include (but are not limited to):

Race; ethnic origin; politics; religion; trade union membership; genetics; biometrics; health, sex life or sexual orientation.

5.5 For more information on data please see the Information Commission Officer's website - **https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/**

6. Data Protection Principles

6.1 Article 5 of the GDPR requires that personal data shall be:

6.1.1 **Processed lawfully, fairly and in a transparent manner** in relation to individuals;

6.1.2 **Collected for specified, explicit and legitimate purposes** 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 purposes shall not be considered to be incompatible with the initial purposes;

6.1.3 **Adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed;

6.1.4 **Accurate and, where necessary, kept up to date**; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

6.1.5 **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 the GDPR in order to safeguard the rights and freedoms of individuals; and

6.1.6 **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.

6.2 These principles apply to every way in which personal data is held or processed, except where an exemption is held, and following these principles is integral to compliance with the requirements of the GDPR. Ultimately the principles protect the interests of the individuals to whom the personal data relates.

6.3 Article 5(2) requires that "the controller shall be responsible for, and be able to demonstrate, compliance with the principles". In all processes and systems of the organisation where data is collected, processed and stored these principles must be adhered to and written procedures should clearly identify the measures put in place to ensure compliance.

6.4 Further information about the principles and guidance is available on the Information Commissioner's Office website or for queries please contact the Director of Resource and Risk Management.

7. Data Processing

7.1 The General Data Protection Regulation defines processing in Article 4 of the General Provisions as:

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

7.2 To summarise this covers any activity carried out with personal data in the work of the organisation. It is important to understand the roles in the processing of data in our organisation and their terms by which they are defined:

Data Subject:	This is the individual to whom the personal data relates.
Data Controller:	YMCA Somerset Coast who is responsible for determining the purposes for which and the manner in which personal data is processed.
Data Processor:	A person or organisation (other than the data controller, data processor or data subject) who processes personal data on behalf of the data controller (for example, but not limited to, the pension provider of the employer's pension scheme).
Third Party:	A person or organisation (other than the data controller, data processor or data subject) who is authorised to process the personal data under the direct authority of the data controller or data processor.
Recipient:	A person, legal person, public authority, agency or other body to whom data must be disclosed whether they are a third party or not.

7.3 In order to process personal data there must be a valid lawful basis for processing. There are six lawful bases for processing set down in Article 6 of GDPR. No single basis is better or more important than another so the one to use will be the most appropriate to the purpose and the relationship with the individual. All processing must be necessary or it will not be compliant under the condition.

7.4 YMCA Somerset Coast requires each area of work to carry out a data audit to map the data required in that area and how it is collected, processed, stored and deleted. This data mapping process allows us to determine the lawful basis for processing and develop and review the privacy notices. All employees are responsible for advising if there are any changes to how data is collected, processed, stored and deleted. Any changes must be notified via email to dataprotection@ymca-sc.org

7.5 The lawful bases are:

7.5.1 **Consent**
Consent means offering individuals real choice and control and requires a positive opt-in. There will be some types of data processing in each area that will require consent and it is important that each manager can easily identify who has and who has not given their consent.

7.5.2 **Contract**
You can rely on this lawful basis if you need to process someone's personal data:

- To fulfil your contractual obligations to them; or
- Because they have asked you to do something before entering into a contract (e.g. provide a quote).

7.5.3 **Legal Obligation**
You can rely on this lawful basis if you need to process the personal data to comply with a common law or statutory obligation. For example (but not limited to) this may be data required by HMRC.

7.5.4 **Vital Interests**

You are likely to be able to rely on vital interests as your lawful basis if you need to process the personal data to protect someone's life.

7.5.5 **Public Task**

You can rely on this lawful basis if you need to process personal data:

- 'In the exercise of official authority'. This covers public functions and powers that are set out in law; or
- To perform a specific task in the public interest that is set out in law.

It is most relevant to public authorities, but it can apply to any organisation that exercises official authority or carries out tasks in the public interest.

7.5.6 **Legitimate Interests**

There are three elements to the legitimate interests basis. It helps to think of this as a three-part test. You need to:

- Identify a legitimate interest;
- Show that the processing is necessary to achieve it; and
- Balance it against the individual's interests, rights and freedoms.

If you choose to rely on legitimate interests, you are taking on extra responsibility for considering and protecting people's rights and interests.

7.6 To process special category data it must be possible to establish a lawful basis under Article 6 of GDPR and in addition to also identify a separate condition for processing special category data as set down in Article 9 of GDPR. There are ten conditions for processing special category data.

7.7 Full details can be found on the Information Commissioner's website - https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/ . However most often in our organisation the appropriate conditions will be either through explicit consent or to protect the vital interests of the data subject. For advice and guidance on this (where lawful basis has not been established) please contact the Director of Resource and Risk Management.

8. Rights of the Individual

8.1 Under GDPR there are eight rights for individual that are set down in the legislation.

8.2 YMCA Somerset Coast holds data on employees, volunteers, customers, suppliers, members, service users and other individuals. It is the expectation of the organisation that all staff who have access to personal data, or who process it as part of their duties, know and understand these rights and how to ensure they are upheld in their area of work.

8.3 The rights of the individual are:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

8.4 **The right to be informed:**

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under GDPR. YMCA Somerset Coast will communicate this information using privacy notices that include the purposes for processing, retention periods and details of anyone we may need to share the data with. Privacy notices must be sent to all individuals at the time that data is first collected.

8.5 **The right of access:**
Individuals have the right to access their personal data and supplementary information. It also allows individuals to be aware of and to verify the lawfulness of the processing.

If an individual makes a request to access their data a copy must be provided free of charge, without delay and within one month. If a request is manifestly unfounded or excessive, particularly if it is repetitive, a reasonable fee can be charged. In extreme circumstances the request can be refused but this must be referred to the Director of Resource and Risk Management before this action is taken and all guidelines from the Information Commissioner's Office must be followed.

It is possible to extend the period of compliance by a further two months where requests are complex or numerous however YMCA Somerset Coast expects this to be rare and if more than one month will be needed the Director of Resource and Risk Management should be notified within one week of receipt of the initial request.

When a request is received the identity of the individual must be verified using "reasonable means". The most appropriate means will depend upon the nature of the records (for example whether a photo is held) and should be recorded with the data access request information. The simplest form of verification will be to ask for two pieces of information including (but not limited to):

- Membership number (Health & Wellbeing)
- Date of birth
- First line of home address
- Postcode
- Normal method of payment

The questions asked will need to appropriate to the area of work and should be approved by the manager of the department.

Copies of the data should be provided in a way that is relevant to the manner in which it is requested. For example, if a request is received by email the data should be provided in electronic format but if the request comes by post then it will be appropriate to send the information to the individual by post. Data security must be maintained whichever method is used. Documents sent by email should be password protected and paper copies should be sent by special delivery or collected in person.

8.6 **The right to rectification:**
This allows individuals to have inaccurate personal data rectified or made complete if it is incomplete. This can be requested verbally or in writing. The request must be responded to within one calendar month.

If the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature, it may be possible to refuse it or to charge a reasonable fee to deal with it. In this case the decision must be referred to the

Director of Resource and Risk Management within one week of receipt of the request and all Information Commissioner's Office guidelines must be followed.

8.7 **The right to erasure:**
This right is also known as "the right to be forgotten". It allows the individual to request that all the personal data held for them be deleted. This right is not absolute and only applies in certain circumstances, as detailed in this link - **https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/**

If an individual makes a valid request the action must be completed within one month and confirmation must be given to the individual. If the request does not meet the required circumstances the individual must be informed with an explanation and details of how to complain to the Information Commissioner's Office. All queries about validity should be referred to the Director of Resource and Risk Management.

8.8 **The right to restrict processing:**
This is where individuals have the right to request the restriction or suppression of their personal data. Again this is not absolute and only applies in certain circumstances, as detailed in this link - **https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-restrict-processing/**
All requests of this nature should be referred to the Director of Resource and Risk Management.

8.9 **The right to data portability:**
This right allows individuals to obtain and reuse their personal data for their own purposes across different services.

In order to be valid the request must meet the requirements detailed on the Information Commissioner's website. The same response times apply as those for a data access request, one month that can be extended by two months in some instances.

The data must be supplied in a structured, commonly used and machine readable form (for example as a CSV file).

8.10 **The right to object:**
An individual has the right to object to the processing of their data and the objection should be assessed to check if it is valid. All objections should be directed to the manager of the department and referred to the Director of Resource and Risk Management as necessary.

Where an objection is found to be valid processing must stop immediately.

8.11 **Rights in relation to automated decision making and profiling:**
YMCA Somerset Coast does not currently operate automated decision making or profiling activities.

8.12 Any requests should be directed to either dataprotection@ymca-sc.org or Data Protection Officer, YMCA Somerset Coast, George Williams Centre, Friarn Avenue, Bridgwater, Somerset, TA6 4RF. Requests will then be forwarded to the appropriate manager for action.

9. Retention Periods

9.1 The data stored by each area of work of the organisation will require different retention periods, varying due to different legal and statutory requirements as well as the purpose of the data.

9.2 YMCA Somerset Coast requires all managers to determine the retention periods of the data their teams work with as part of the data mapping process, to be agreed by the senior manager of the area of work. Where legal or statutory requirements apply these must be clearly stated. If there is no specific legal or statutory requirement the retention period must be determined on a reasonable basis that is clearly articulated in the data mapping records.

9.3 Due to the charitable status of the organisation all financial data must be kept for seven years for Charity Commission audit purposes.

9.4 Electronic data must be deleted at the point that the retention period expires. The manager of each team is responsible for ensuring that this has been completed.

9.5 Paper records must be destroyed through secure means by a contractor appointed by the organisation. A certificate of safe destruction must be held on file. All paper records must be safely transported to the collection point in boxes clearly labelled with the contents and date to be destroyed. From the collection point external contractor will collect the files to be stored in secure offsite storage.

9.6 Appendix 1 lists suggested retention periods. Managers should advise the Director of Resource and Risk Management of any amendments required.

10. Breaches

10.1 A personal data breach is a breach in security of data that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data. This means that all incidents where personal data may become available to people who are not authorised to have access to it will be deemed a breach, whether the incident is accidental or intentional.

10.2 All managers must ensure that staff are sufficiently trained that they understand which data they may access or process through their duties is personal and how it must be kept secure. All staff must also understand who they are authorised to give out personal data to and how they can verify the identity of the individual. Queries should be escalated in line with the accountability section of this policy.

10.3 All breaches must be referred to the Director of Resource and Risk Management immediately upon detection and will be assessed to establish the likelihood and severity of the resulting risk to the individual's rights and freedoms. If the breach is deemed as having the potential to negatively impact the individual the breach will be reportable to the Information Commissioner's Office.

10.4 Reportable breaches must be notified to the ICO without undue delay and within 72 hours of the incident.

10.5 **Breach Procedure:**

- Immediately upon detection of a breach, or possible breach, details of the incident should be reported to the Director of Resource and Risk Management, copying in the manager and senior manager.
- The risk to the individual will be assessed by the Director of Resource and Risk Management.
- If reportable the Director of Resource and Risk Management will contact the ICO with details of the breach, a description of the likely consequences and

confirmation of any measures taken already or to be implemented to deal with the breach.

- Measure to mitigate the risk and to prevent the reoccurrence of such an incident will assessed by the Director of Resource and Risk Management and senior manager of the area of work and will be put in place as soon as possible
- Where the risk to the individual is "high" they will also be informed as soon as possible by the Director of Resource and Risk Management.
- All risks will be recorded whether or not they are reportable.
- All breaches or potential breaches will be investigated by the R Director of Resource and Risk Management and the senior manager of the area of work.
- Actions will be taken to increase security such as immediate changing of passwords, changing of locks or location of keys, staff training or other actions.
- The Human Resources department must be informed by the line manager of the team in which the breach took place and disciplinary proceedings will be commenced if appropriate.

10.6 All stages of implementation of the procedure must be documented along with the reasoning for all decisions taken during the process.

11. CCTV

11.1 Images of people are covered by the General Data Protection Regulation and so is information about people which is derived from images.

11.2 YMCA Bath Group uses CCTV in many of the locations of our work. The images taken in this CCTV are subject to the conditions of the General Data Protection Regulation and must be protected appropriately.

11.3 Access to CCTV images should be by authorised employees only (with password protected access) and training should be given to ensure it is used and managed properly. All departments where CCTV is in operation should have a CCTV procedure to detail who is able to access the images, details of the authorised use of those images and who is responsible for overseeing the use of the system.

11.4 Overall control of the CCTV of the organisation as a whole is held by the Chief Executive.

12. Social Media

12.1 YMCA Somerset Coast uses social media to promote our work, build relationships and raise our profile. All content uploaded to social media must be carried out by authorised members of staff only and the accounts must have designated management and password controlled access. All requests and queries should be sent to the Marketing, Engagement & Events Co-ordinator

.

12.2 Use of images of individuals or other personal data must have prior consent. This can either be written consent or verifiable verbal consent as below:

- Consent confirmed in the signed privacy notice.
- Consent given by letter or other written format.
- Verbal consent (for example in a group photo where it is clearly communicated that the image will be for social media before the image is taken) recorded in writing.

12.3 The manager of each department is responsible for ensuring that consent has been given for all individuals who appear in a recognisable way in a photo, or who give a quote or other data that may be used. Once consented to, the data is only consented

for the use by the organisation and must not be used on a personal basis by any member of staff. To use images on personal social media would be a breach of General Data Protection Regulation and may be subject to disciplinary proceedings.

12.4 It is possible to share or comment on social media posts of the organisation as with other social media posts. All employees must remember to uphold the integrity and professionalism of the organisation when doing so.

12.5 It is recommended that employees of the organisation do not accept or initiate "friend" requests from service users of the organisation on a personal basis.

13. Employment

13.1 YMCA Somerset Coast must process personal information for the purposes of recruitment, selection and employment of staff for the organisation. Throughout this process the organisation ensures compliance with the eight principles of data protection.

13.2 Where an individual makes an application for a role with YMCA Somerset Coast Group, either for paid employment or on a voluntary basis, the processing of their personal data is necessary for the consideration of their application. The personal data is given freely and with consent by the individual. YMCA Somerset Coast Group will only use this data for the purposes of recruitment and selection. A privacy notice will be issued to applicants to all posts.

13.3 Once a successful appointment has been made the processing of personal data becomes necessary to the performance of the contract of employment. Personal data held and processed by the Human Resources and Payroll departments of YMCA Somerset Coast Group will by nature at times be classes as sensitive personal data.

13.4 Sensitive personal data may only be requested and/or processed where one or more of the conditions for processing are met and security of this data is considered paramount by the organisation.

13.5 From time to time YMCA Somerset Coast Group may ask employees for consent to use information such as names, photographs or other general information to use on our website or in marketing material. In this event consent will be requested either in writing or verbally and the data will only be used if freely given.

13.6 Employees and volunteers are entitled to view the information held on them at any time under a data access request therefore files should be kept up to date and in a form that complies with the requirements in the event of a request being made.

13.7 Disclosure of personal data to someone other than the data subject must comply with the requirements of General Data Protection Regulation. This means that either consent must be given by the data subject or it must be covered by requirement such as, but not limited to, a legal obligation. If data is shared without consent and no other lawful basis is valid this will be treated as a breach and in some circumstances may result in disciplinary proceedings.

13.8 All queries should be directed to the Director of Resource and Risk Management.

14. General Procedure

14.1 YMCA Somerset Coast requires each department to have a specific data protection procedure however these general items apply to all areas of work.

14.1.1 Training in Data Protection must be incorporated into the induction of each employee or volunteer to ensure a good understanding of the requirements of this policy – this may be on a one to one basis with the policy or additional training may be provided if required.

14.1.2 All personal data must be stored and processed in line with this policy and must comply with the requirements of General Data Protection Regulation.

14.1.3 All individuals whose data will be processed must be given a privacy notice at the time of collection of the data or before the data is collected.

14.1.4 All privacy notices must be kept on file for the duration of processing and retention of the personal data.

14.1.5 Details of lawful processing must be recorded and adhered to.

14.1.6 Personal data collected must be compliant with the principles of data protection and managers must evaluate any forms or other documentation to ensure that unnecessary is not requested as this would be a breach of data protection.

14.1.7 Storage of personal data must be secure at all times and only authorised employees should have access to the data – this may involve locked cabinets, key safes or passwords among other methods – passwords, keys or codes must not be shared.

14.1.8 Any personal data held on computerised systems should be accessible with passwords for named individuals or teams and should not be shared with anyone else.

14.1.9 Time limits for the storage of personal data that is no longer being processed must be defined on a statutory or reasonable basis, as applicable, by the senior manager of each area of work and once the allotted time has passed the personal data must be destroyed, deleted or returned securely.

14.1.10 Requests for personal data by anyone other than the data subject must be carefully handled to ensure that data protection is not breached – queries about the lawful basis for the request must be escalated as detailed in the Accountability section of this policy.

14.1.11 Validity of a request for personal data must always be checked to ensure that all reasonable steps are taken to ensure it is not a fraudulent request – queries about this must be escalated as detailed in the Accountability section of this policy.

14.1.12 Breaches of data protection at any level must be reported to the Manager, Senior Manager and Human Resources Department and could lead to disciplinary proceedings.

14.1.13 Failure to report a breach of data protection must also be reported to the Manager, Senior Manager and Human Resources Department and could also lead to disciplinary proceedings.

15. Accountability

15.1 **Every employee is accountable for:**

15.1.1 Understanding the requirements of General Data Protection Regulation and ensuring compliance with this policy.

15.1.2 Maintaining security of personal data held by the organisation and accessible within their role.

15.1.3 Using personal data for the performance of their role under the conditions required to carry out their work and in line with the principles of data protection.

15.1.4 Only accessing data for which they are authorised and referring to a line manager where greater authorisation is required.

15.1.5 Issuing personal data only where the validity of the request has been checked and the person making the request is either the data subject, the data subject has given consent for the release of the information to the person making the request or there is another lawful basis such as a legal obligation.

15.1.6 Maintaining the security of keys, codes to key safes, computer logins and any other security measure that limits the access to data to authorised personnel only.

15.1.7 Storing data only in secure locations or using secure devices appropriate to the use and within the requirements of General Data Protection Regulation and this policy.

15.1.8 Escalating queries to the line manager if they have any doubt about whether to give out information.

15.1.9 Reporting breaches of data protection to the manager of the department, senior manager and Director of Resource and Risk Management.

15.1.10 Ensuring security of passwords and access details both in IT and physical storage.

15.1.11 Issuing privacy notices to any individual whose data they are collection as part of the performance of their job role.

15.2 **The Line Manager is accountable for:**

15.2.1 Ensuring their teams are aware of this policy through induction and training.

15.2.2 Requesting additional training where required for members of their teams or for themselves.

15.2.3 Understanding the requirements of General Data Protection Regulation and ensuring compliance with this policy.

15.2.4 Ensuring that privacy notices are issued to all individuals whose data will be collected and processed and that appropriate consent is obtained where necessary.

15.2.5 Maintaining security of personal data held by the organisation and accessible within their role.

15.2.6 Preparing for individuals' data access requests and ensuring that all members of the team know how to verify the identity of the person making the request.

15.2.7 Ensuring security of passwords and access details both in IT and physical storage.

15.2.8 Using personal data for the performance of their role under the conditions required to carry out their work and in line with the principles of data protection.

15.2.9 Only accessing data for which they are authorised and referring to a senior manager where greater authorisation is required.

15.2.10 Issuing personal data only where the validity of the request has been checked and the person making the request is either the data subject, the data subject has given consent for the release of the information to the person making the request or there is an another lawful basis such as a legal obligation.

15.2.11 Maintaining the security of keys, codes to key safes, computer logins and any other security measure that limits the access to data to authorised personnel only.

15.2.12 Escalating queries to the senior manager if they have any doubt about whether to give out information.

15.2.13 Reviewing forms and other documentation to ensure that the data collected is compliant with the principles of data protection.

15.2.14 Reporting breaches of data protection to the senior manager of the area of work and the Director of Resource and Risk Management.

15.2.15 Supervising the storage of data and ensuring that data is deleted/destroyed in accordance with this policy when the retention period has expired.

15.3 **The Senior Manager is accountable for:**

15.3.1 Ensuring their teams are aware of this policy through induction and training.

15.3.2 Requesting additional training where required for members of their teams or for themselves.

15.3.3 Understanding the requirements of data protection and ensuring compliance with this policy.

15.3.4 Maintaining security of personal data held by the organisation and accessible within their role.

15.3.5 Using personal data for the performance of their role under the conditions required to carry out their work and in line with the principles of data protection.

15.3.6 Only accessing data for which they are authorised.

15.3.7 Issuing personal data only where the validity of the request has been checked and the person making the request is either the data subject, the data subject has given consent for the release of the information to the person making the request or there is an exemption such as a legal obligation.

15.3.8 Maintaining the security of keys, codes to key safes, computer logins and any other security measure that limits the access to data to authorised personnel only.

15.3.9 Escalating queries to the Director of Resource and Risk Management if they have any doubt about whether to give out information.

15.3.10 Reviewing forms and other documentation to ensure that the data collected is compliant with the principles of data protection.

15.3.11 Reporting breaches of data protection to the Director of Resource and Risk Management.

15.3.12 Ensuring security of passwords and access details both in IT and physical storage.

15.3.13 Checking that each team has appropriate and robust procedures that are compliant with this policy and GDPR guidelines for storing data and deleting/destroying data when retention periods expire.

15.4 **The Chief Executive and Director of Resource and Risk Management are accountable for**:

15.4.1 Ensuring that adequate policies and procedures are created for the organisation.

15.4.2 Ensuring that training resources and/or sessions are provided as required.

15.4.3 Understanding the requirements of General Data Protection Regulation and ensuring that the organisation operates in compliance with those requirements.

15.4.4 Ensuring that any serious breaches of data protection are reported and dealt with appropriately.

15.4.5 Assessing incidents that may have caused a breach (Director of Resource and Risk Management).

15.4.6 Reporting breaches to the Information Commissioner's Office as appropriate (Director of Resource and Risk Management).

15.5.7 Keeping records of all incidents that may have caused a breach (Director of Resource and Risk Management).

15.5.8 Ensuring that membership of the Information Commissioner's Office is maintained.

15.5.9 Providing adequate secure storage for personal data.

15.5.10 Appointing a contractor for the secure destruction of paper records and storing certificates.

15.5.11 Ensuring security of passwords and access details both in IT and physical storage.

16. Queries

16.1 If there are any queries relating to this policy please contact the Risk & Development Manager.

17. Responsibility

17.1 The Director of Resource and Risk Management is responsible for the effective implementation of this policy.

18. Monitoring and Review

18.1 We will monitor the volume and frequency of information requests and breaches and report regularly to the Board. The policy will be reviewed every three years or sooner subject to changes in legislation.

Reference: Bath YMCA GDPR Policy