YMCA Fairthorne Group

Policy Level	Two
Policy Category	Business
Policy Authority	Senior Leadership Team
Lead Committee	Senior Leadership Team
Lead Director	Emma Corina
Approved Date	07/10/2018
Review Date	29/02/2020

Data Protection & Information Security Policy

YMCA Fairthorne Group (YMCA) recognises the requirements placed upon it by the General Data Protection Regulation (GDPR) and data retention legislation to receive, record, organise, store, protect and destroy data concerning its clients, employees and volunteers.

The GDPR purpose is to protect an individual's rights and freedoms and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

YMCA will abide by the GDPR principles of:

- lawfulness, fairness and transparency
- purpose limitation
- data minimisation
- accuracy
- storage limitation
- integrity and confidentiality.

Governance, Compliance and Accountability

- YMCA is a data controller and data processor under the GDPR. The trustees, senior leadership and managers are responsible for developing and encouraging good information handling practices within the organisation.
- We have appointed a Data Protection Officer (DPO) who has responsibility for the overall supervision, implementation and ongoing compliance with the data protection laws. The DPO will have the relevant skills and resource to fully implement this policy.
- Compliance with data protection legislation is the responsibility of all employees who process personal data and forms part of the YMCA induction, training and performance management process. Employees are responsible for ensuring that any personal data about them and supplied by them to the YMCA is accurate.
- Each organisation function is monitored for compliance, review and improvement with regards to GDPR regulations.
- We monitor the Supervisory Authority and GDPR news and updates, to stay abreast of updates, notifications and additional requirements
- We have robust and documented Complaint Handling and Data Breach controls for identifying, investigating, reviewing and reporting any breaches or complaints with regards to data protection
- We have developed and documented appropriate technical and organisational measures and controls for personal data security

Rights

All customers, employees and potential employees have the following rights concerning their data:

1. **To be informed** - about the collection and use of your personal data at the time we collect the data, the recipients to whom the personal data has/will be disclosed, why we

process your data, how long we store it for, who has access to it and who we share it with.

2. **To have access** to any personal information that YMCAFG processes about you and confirmation that your data is being processed so you can verify the lawfulness of the processing.
3. **To rectification** - we will update inaccurate information that you tell us about either verbally or in writing.
4. **To erasure** - of your personal data in accordance with data protection laws, as well as to object to any direct marketing from us and to be informed about any automated decision-making that we use.
5. **To restrict processing** – of your personal data. We may retain the data in accordance with data protection laws, but not use it.
6. **To data portability** – allowing you to obtain and reuse your personal data for your own purposes across different services.
7. **To object** – to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority, direct marketing and processing for purposes of scientific/historical research and statistics.
8. **Not to be subject to automated decision-making profiling** – where automated decisions are made without any human involvement.

If we receive a request to exercise any of the above rights, we may ask for verification of identity before acting on the request; this is to ensure that data is kept protected and secure. To exercise rights, contact should be made with YMCA via any communication channel or via the Contact Us section of our website www.ymca-fg.org.

All requests to exercise rights will be given to the DPO, who will oversee all related investigation and resulting changes. The request, decisions and related activities will be documented in the GDPR area of Sharepoint.

Privacy Notice

A privacy notice outlines how, why and when we gather and process personal information in compliance with the relevant data protection regulation, as well as providing an outline of the necessary information regarding rights and obligations. YMCA has the following privacy notices for the collection and processing of personal data:

- Customer Privacy Notice – relating to customers and recipients of YMCA services
- Staff Privacy Notice – relating to current and former employees and volunteers
- Recruitment Privacy Notice – relating to job applicants.

All YMCA privacy notices are on our website and the YMCA SharePoint site. Privacy notices are referred to in relevant correspondent to the above groups.

Documenting Lawful Basis

When we process personal data, we always identify and establish the legal basis for doing so. This is determined by the purpose and relationship with the individual:

a) Consent to the processing of their personal data for one or more specific purposes
b) Deliver a contract or to take steps to deliver a contract e.g. to provide a quote.
c) Protect the vital interests of a data subject e.g. providing medical information in an emergency.
d) Legal obligation e.g. informing OFSTED of an incident
e) Legitimate interests e.g. where people would expect us to process data, such as a Daycamp booking for a child
f) Special category data – see below

The lawful basis for the data identified in our privacy notices is documented in a spreadsheet called Lawful Basis which is stored in the GDPR section of Sharepoint.

Consent

YMCA understands consent to mean that it has been explicitly and freely given by statement or a clear affirmative action, signifying agreement to the processing of personal data.

- Consent is required when no other lawful basis applies.
- Consent will always be sought but if consent is not in place and other lawful basis applies, YMCA will still take action.
- In most instances, consent to process personal and sensitive data is obtained routinely using standard consent documents e.g. booking conditions for a service.
- For sensitive data, explicit written consent must be obtained unless an alternative legitimate basis for processing exists.
- Consent can be withdrawn at any time.
- Consent is stored on the relevant processing software and/or YMCA SharePoint.
- Where processing relates to a child under 13 years old, consent must be given by the person with parental responsibility for the child. YMCA will demonstrate reasonable efforts to verify the age of the child and establish the authenticity of the parental responsibility. YMCA will use the Fraser Gillick Competency guidelines to determine a child's capacity to consent, including the consideration of balancing a child's rights with our responsibility to keep children safe from harm.

Special Category Data

Special category data is personal data which is more sensitive and therefore requires more protection. Data will only be collected and processed where we have explicit consent under one of the following conditions:

1. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
2. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
3. processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
4. processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
5. processing relates to personal data which are manifestly made public by the data subject;
6. processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
7. processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

8. processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
9. processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
10. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Data Breaches

A personal data breach is defined as a security incident that has affected the confidentiality, integrity or availability of personal data. A personal data breach occurs when:

- any personal data is lost, destroyed, corrupted or disclosed
- if someone accesses the data or passes it on without proper authorisation
- if the data is made unavailable e.g. when it has been encrypted by ransomware, or accidentally lost or destroyed.

If a security incident takes place, we will establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including informing the ICO if required.

Detecting & investigating a data breach

We perform regular checks and assessments on how the personal data we process is obtained, used, stored and shared to prevent data breaches. If a data breach is detected, the following steps are followed:

1. The DPO must be immediately using any communication method. The DPO will request this be followed up in writing.

2. The DPO will assess the immediacy and severity of the situation, and will either make a decision or commission an investigation, which will be led by a senior member of staff. Where immediate action needs to be taken, DPO will instruct this, including changes to procedures if necessary.

3. Investigation findings will include recommendations which will be the responsibility of the director team to implement.

4. The DPO will log the breach in the Data Breach Log and file copies of related correspondence.

5. The DPO will identify whether the ICO should be informed (required within 72 hours).

When & how to inform the ICO of a data breach – if a personal data breach has occurred, the DPO will assess the potential negative consequences for individuals:

- if there is a risk to people's rights and freedoms, the risks will be justified and documented and we will contact the ICO.
- Breaches must be reported within 72 hours of the breach. Contact the ICO on 0303 1231113 or visit https://ico.org.uk/for-organisations/report-a-breach/
- If there is no risk, the breach will be documented but not reported.

Further guidance regarding data breaches can be found at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/.

Data Protection Impact Assessment (DPIA)

YMCA uses a Data Protection Impact Assessment (DPIA) to identify and minimise the data protection risks of a project. Such projects are likely to result in a high risk to individuals or any major project which requires the processing of personal data. A DPIA consists of:

- Screening questions to identify if a DPIA is required
- Project brief – detailing the what, how and why of the project that will process personal data and sets out the outcomes, intentions and risks.
- Information audit to assess where personal data comes from, goes to and how it is processed
- Assessment criteria to provide the basis for identifying the risks and specific details such as how the data is used, if it is disclosed or transferred and what privacy by design methods are in place.
- Privacy issues & risks
- Proposed solutions & mitigating actions
- Integrating outcomes - specifying the actions to be taken, who is responsible and what the completion timeframe is.

Once the DPIA is completed we will reassess the project to ensure that it meets the regulation requirements.

Privacy by design & information storage

Information Storage

Information is stored on a long-term basis in the following formats:

- Documents on a secure file server via Microsoft SharePoint
- Housing information on AMIS via Azure
- Nursery information on Connect
- Customer information on NetSuite CRM
- Emails (see Information Distribution, below)
- Staff information on Access SelectHR
- Spreadsheets contained in secure areas of Sharepoint, to be used only for data which cannot be used in the above system.

This information is backed up either in Azure or other hosted environments using secure methods in the UK, or in the case of NetSuite, the EEA. No personal information should be stored locally on PCs or desktops.

- Paper - all paper-based information is kept in lockable storage in locked rooms with access provided to nominated suitable persons only. Paper based information is subject to procedures for storage length, archiving and destruction.

Information may be stored on a short-term basis in the following formats:

- Approved portable PCs such as YMCA issued laptops and smart phones. Senior staff and staff with access to sensitive data outside of the YMCA network access data using multi-factor authentication. Files stored locally on YMCA laptops are encrypted. Such equipment have a password protected lock or log in.
- Paper-based for the purposes of assessment, supervision and meetings.

When such devices contain information they must be kept in a locked safe when not in direct use and the information deleted immediately it is no longer needed.

A separate record summarising the type of information that is stored on these devices should be kept in case of data theft (see below).

- Access is restricted to shadow IT to ensure data is not transferred outside of our network via personal accounts.
- USB or thumb drives are not permitted at the YMCA for reasons of data security and virus protection.

Information Distribution

Internal distribution

Information should only be shared with members of staff who have a direct interest in the content and where the content is directly relevant to their work.

Internal sharing of information should be done using permissions access for approved systems only. This means that any files or folders in any system should be accessible by approved persons only, and the information itself should not be distributed outside of those systems. Please refer to each service's confidentiality operating procedures.

On occasion it may be required to send information within the organisation by email. This should be done using the minimum information required and referring the recipient to the relevant file location. On no occasion should information be distributed using BCC function in email.

External distribution (Data Transfers)

Data is only transferred for legal and necessary purposes, utilising a process that ensures such data is encrypted with a secret key and where possible is also subject to data minimisation. It is the responsibility of each manager to ascertain whether information should be shared with an external agency, in consultation with the DPO.

We use approved, secure methods of transfer. All data being transferred is noted on our information audit so that tracking is easily available, and authorisation is accessible.

Data held on electronic systems

Personal data of employees in network systems, computer systems, communication equipment used by employees, access controls and other internal management / administration is not subject to minimum or maximum retention requirements.

All data stored externally is encrypted and password protected. Security permissions are set for all electronic data access.

Connect, AMIS and Sharepoint are all stored on an external datacentre contracted via an external IT support company. Records are backed up overnight and kept for 30 days after which they are overwritten.

Netsuite is stored on an external mirrored datacentre contracted via an external IT support company and backed up every day. YMCA puts data out of use via local file deletion.

Records of Processing Activities

YMCA maintains records of all processing activities and our internal records contain the following information:

- Our full name and contact details and the name and contact details of the Data Protection Officer.
- The purposes of the processing
- A description of the categories of data subjects and of the categories of personal data
- The categories of recipients to whom the personal data has or will be disclosed
- Where possible, the envisaged time limits for erasure of the different categories of data
- A general description of the processing security measures

Third Party Processors

The YMCA uses external processors for certain processes. Such external processing includes (but is not limited to):

- IT Systems and Services
- Legal Services
- Debt Collection Services
- Human Resources

We have strict due diligence procedures in place and review, assess and background check all processors prior to forming a business relationship. We obtain company documents, references and ensure that the processor is adequate, appropriate and effective for the task we are employing them for. We check privacy notice, data protection and GDPR compliance and require non-disclosure and/or service level agreements where appropriate.

Automated Decision-Making

YMCA does not undertake any automated decision making.

Data Retention

1. **Data Retention**[1]

The Information Commissioner obliges us to:

- adhere to all of the rights of the GDPR
- review the length of time we keep personal data (including taking into account document retention requirements under UK law and individual contracts)
- consider the purpose or purposes we hold information for in deciding whether (and for how long) to retain it

[1] Source: Iron Mountain Document Retention Guide UK

- securely delete information that is no longer needed for this purpose or these purposes
- update, archive or securely delete information if it goes out of date.

Relevant legislation

- General Data Protection Regulations
- Companies Act 2006
- Limitation Act 1980
- VAT Act 1994
- Taxes Management Act 1970
- Income Tax (PAYE) Regulations 2003
- Finance Act 1998
- Corporation Tax Act 2010
- Customs and Excise Management Act 1979
- Money Laundering Regulations 2007
- Registered Pension Scheme (Provision of Information) Regulations 2006
- Control of Substances Hazardous to Health Regulation 2002
- RIDDOR Regulations 2013
- SI 1986/1960, SI 1982/894, SI 2003/2682, SI 1998/1833
- National Minimum Wage Act 1998, National Minimum Wage Regulations 1999

General Company Records

All business contracts, agreements and arrangements will be stored for the length of the contract and for a period of 6 years afterwards. Records are retained on an electronic database and paper copies in locked storage.

Pension records will be stored for an indefinite period, and a minimum of 6 years.

VAT records will be stored for an indefinite period, and a minimum of 6 years.

Company accounts are kept for an indefinite period. Records are retained on an electronic database.

Board meeting minutes, resolutions, and details of company directors are kept for an indefinite period. Records are retained on an electronic database.

HR records

All financial records including payroll and salary[2], sickness[3], maternity pay[4], PAYE and pension[5] may be kept indefinitely. Records are retained on an electronic database.

All employment contract records, training records, written particulars of employment, identification documents, changes to terms and conditions, working time regulations, correspondence and other agreements between YMCA and an employee are kept for a minimum period of 3 years and a maximum period of 6 years after termination of employment, after which they are put beyond use.

[2] Minimum 6 years for purpose of tax returns
[3] Minimum 3 years
[4] Minimum 3 years
[5] Minimum 3 years

Data of rejected job applicants will be put beyond use or destroyed, unless the applicant wishes to remain on file for future posts.

Customer and Member Records

Customers have the opportunity to unsubscribe or amend marketing preferences with every communication. Customer accounts that have not been used for 5 years are made inactive and personal information we are not required by law to retain, will be put beyond use.

Nursery

Children's records will be kept for a period of 3 years after they have left the nursery[6]. This includes registers, accident and incident forms, learning journeys, and other records as required to deliver the EYFS. Children's Learning Journeys will be shared with the school the child is transitioning to in electronic form. These files are stored on our online system, Sharepoint, and paper copies are destroyed within 12 months of a child leaving nursery.

Please see below regarding safeguarding records.

Daycamps

Children's records will be kept for a period of 3 years after they last attended Daycamps. This includes registers, accident and incident forms, safeguarding files, and investigation reports. These files are stored on our online system, Sharepoint, and paper copies are destroyed.

All accident reports are kept until child reaches the age of 21, or indefinitely in the case of a child with a disability.

Group visits

Children's records will be kept for a period of 3 years after they attended with their group. This includes accident and incident forms, rooming lists, dietary requirements, safeguarding files, and investigation reports. These files are stored on our online system, SharePoint, or NetSuite CRM. Paper copies are destroyed.

Housing

We are obliged to retain housing resident records for a period of 7 years after they have moved out. Records are stored electronically for a period of 7 years, then put out of use through deletion. Paper based records are archived by scanning to SharePoint in folders labelled with a destroy date. Paper records are destroyed.

All accident reports are kept until young person reaches the age of 21, or indefinitely in the case of a young person with a disability.

Support services (e.g. young carers, support in housing, youth services)

Records are kept for a period of 3 years after the person last accessed the service. This is because service users often return to the service after having left for a period of time.

Paper based records are archived by scanning to SharePoint in folders labelled with a destroy date. Paper records are destroyed. Electronic database records are put out of use by local deletion.

[6] EYFS Guidance

All accident reports are kept until child reaches the age of 21, or indefinitely in the case of a child with a disability.

Health and safety

Medical and safety records for employees under health surveillance will be kept indefinitely, and for a minimum of 40 years, if the employee has worked under dangerous conditions, come into contact with substances hazardous to health, including biological agents, asbestos and radiation. These records will be kept separate to HR and finance records.

RIDDOR records will be kept indefinitely, and for a minimum of 3 years.

Safeguarding

Any records relating to safeguarding will be kept indefinitely, or until/unless a formal inquiry requests their disposal. This includes case files and investigation notes.[7] All records will be stored electronically and paper copies destroyed.

2. Data held on electronic systems

Personal data of employees in network systems, computer systems, communication equipment used by employees, access controls and other internal management / administration is not subject to minimum or maximum retention requirements.

All data stored externally is encrypted and password protected. Security permissions are set for all electronic data access.

All data is stored at external data centres contracted via external IT support companies. Contracts with support companies describe how they are compliant with GDPR or records of their privacy notice and/or data protection policy are checked and retained. Records are backed up overnight and kept for 30 days after which they are overwritten. YMCA puts data out of use via local file deletion.

Hardware data destruction

Hardware is taken to a computer company which erases all remaining information on the hard disk using software approved by CESG, to the Infosec 5 standard. Certificates are obtained.

Reference

The embedded guide has been used as a reference source for this policy.

Document Retention Guide.pdf

[7] We have adopted the guidance from the IICSO Inquiry