

***YMCA St Helens***

***Confidentiality and Personal Data Policy and Procedure***

This is an important document because it contains details of:

**How YMCA St Helens meets the requirements of the General Data Protection Regulations**

If you find this policy difficult to understand please talk to one of the YMCA Management Team

***YMCA St Helens***

***Confidentiality and Personal Data Policy & Procedure***

**Introduction**

YMCA St Helens will adhere to General Data Protection Regulations

(GDPR coming into force on 25th May 2018) and Computer Misuse

Act 1990 in relation to maintaining the Confidentiality and Personal

Data Policy and Procedure.

**Purpose**
YMCA St Helens is committed to being transparent about how it collects and uses personal data, and to meeting its data protection obligations. This policy sets out the organisation's commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of job applicants, employees, workers, contractors, volunteers,  and former employees, referred to as HR-related personal data.

This policy applies to the personal data of clients or other personal data processed for business purposes.

The organisation has appointed Sarah Challands; Operational Director as the person with responsibility for Data Protection compliance within the organisation. You can email her at: sarah.challands@sthelensymca.org.uk

Questions about this policy, or requests for further information,

should be directed to her.

**Definitions**

"Personal data" is any information that relates to an individual who

can be identified from that information. Processing is any use that is

made of data, including collecting, storing, amending, disclosing or

destroying it.

"Special categories of personal data" means information about an

individual's racial or ethnic origin, political opinions, religious or

philosophical beliefs, trade union membership, health, sex life or

sexual orientation and biometric data.

"Criminal records data" means information about an individual's

criminal convictions and offences, and information relating to

criminal allegations and proceedings.

Computer Misuse Act 1990 in summary states it is an offence to

gain unauthorised access to a computer system. This includes

causing a computer to perform a function with intent to secure

access to any program or data, knowing that the access is

unauthorised. This is an offence regardless of whether the motives

for access were well-meaning or malicious. Access to any program

or data held in a computer system is a wide definition which

includes – altering or erasing programs or data, copying it, moving

it, using it and having it output from the computer in which it is

held. Examples of such offences could include – unauthorised use

of another person’s user name or password, persistently trying to

guess a user name or password and laying a trap to obtain a

password of password file.

**Data Protection Principles**
The organisation processes personal data in accordance with the following data protection principles:

The organisation processes personal data lawfully, fairly and in a transparent manner. To ensure data is ‘fairly and lawfully processed’ you will be advised who is collecting, holding, and accessing the data, and for what purposes.

The organisation collects personal data only for specified, explicit and legitimate purposes.

The organisation processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.

The organisation keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay. In relation to the accuracy of HR records this shall be ensured by at least an annual review ensuring up to date information is maintained.

The organisation keeps personal data only for the period necessary for processing. All records deemed to be obsolete will be destroyed, providing legal obligations are met regarding the retention of information.

The organisation adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage. Security of HR records shall be ensured by the use of Password protected computer records, locked filing cabinets with specific key-holders and only specific personnel shall have access. An employee’s personal data will not be removed from the HR department unless authorised by the Audit Committee.

The organisation tells individuals the reasons for processing their

personal data, how it uses such data and the legal basis for

processing in its privacy notices. It will not process personal data of

individuals for other reasons.

Where the organisation processes special categories of personal

data or criminal records data to perform obligations or to exercise

rights in employment law, this is done in accordance with a policy

on special categories of data and criminal records data.

The organisation will update personal data promptly if an

individual advises that his/her information has changed or is

inaccurate.

Personal data gathered during the employment, worker, contractor

or volunteer relationship, or apprenticeship or internship is held in

the individual's personnel file (in hard copy or electronic format, or

both), and on HR systems. The periods for which the organisation

holds HR-related personal data are contained in its privacy notices

to individuals.

Personal data gathered during the assessment or the provision of:

Activities, Accommodation or Childcare services is held on an

individual's file (in hard copy) , and on related computer systems.

The periods for which the organisation holds personal data are

contained in its privacy notices to individuals.

The organisation keeps a record of its processing activities in

respect of personal data in accordance with the

requirements of the General Data Protection Regulation (GDPR).

**Individual Rights**
As a data subject, individuals have a number of rights in relation to their personal data.

**What Information is Collected & Held**

In respect of employees:

* Original application and accompanying documents related to the employment process such as CV’s, references, interview notes, or materials connected with the selection processes.
* Personnel Action forms or notices of pay change and any accompanying documentation
* Performance reviews, supervision notes and performance appraisal documentation
* Letters of commendation or complaint connected with employment
* Promotional opportunity application and related materials
* Documents submitted by the employee such as birth certificates, training certificates, Identification Certificates e.g. passport, driving licence.

In respect of clients:

* Original application and accompanying documents related to the application process, including reports from third parties.
* Reports relating to care, support, health & safety, education etc to ensure appropriate person centred service delivery

**How Information is Collected**

YMCA St Helens collects information in the following ways:

* Personal request direct from residents, members, users or employees.
* Reports requested from external agencies with consent of clients, etc

CCTV is in operation in all public areas with the exception of toilets and changing facilities. The recordings are for genuine safety and security purposes and signs around the premises highlight its usage to all. The recordings are kept in secure areas and locked away at all times with restricted access. The recordings may be used in supporting evidence in the event of any incident.

The Association reserves the right to monitor employees’ internal and external e-mails and use of the Internet, both during routine audits of the computer system and in specific cases where a problem relating to excessive or unauthorised use is suspected.

**What the Information is Used For**

The information given to staff is used in a variety of ways including

more specifically:-

1. Assessing applications e.g. accommodation, childcare services, training, membership etc;
2. Ensuring that support, care etc are appropriate for the individual
3. Ensuring that correct appropriate information is given to the Benefits Agency and other agencies, and lessening administration delays
4. Assisting staff in establishing that appropriate accommodation and support are being given to an individual
5. That in given situations the right people are contacted, e.g. Medical Aid or Next of Kin;

f) Management and day to day usage of personnel information for all new, current and past employees.

Access to information is deliberately limited to the people who require it. The only people to have access to the above information will be:-

1. YMCA Housing Team or Programme Co-ordinators, as

appropriate;

 b) Administrative personnel;

 c) Chief Executive or Operational Director (or Senior

 Manager in charge);

1. Beacon Nursery Manager, Housing Services Manager, departmental heads
2. Committee Members (in the form of reports).

**Disclosure of Information to Third Parties**

Confidentiality means that information is held in trust by those

employed by the YMCA, volunteers working for the YMCA or

Committee Members of the YMCA and is not disclosed without prior

permission from residents, clients, members or employees to

parties other than:

a) The Benefits Agency and other agencies specifically to aid benefit claims being made;

b) The Local Authority specifically in respect of housing benefit payments and re-housing applications, Funding Team in respect of childcare provision,

c) Agencies specifically invested in the care of children eg Ofsted, Social Services, including the Disability Team, Bridge Centre Speech and Language, Physiotherapy services, children’s centres, health visitors . etc.

d) The police when involved in a criminal investigation or to serve a warrant and the Adult Safeguarding Team, again when involved in an investigation.

e) Agencies specifically invested in the support of housing clients e.g. CGL etc

Information should never be disclosed without an individual’s

permission and should not be given out over the telephone to

callers. Verification should be obtained as to the identity of callers

when purporting to be from outside agencies; wherever possible

staff from public agencies will be asked to either call in personally or

write in with requests for information.

Information held by the YMCA and details of the names and

addresses of residents, members or employees will not be divulged

to members of the public, whether purporting to be relatives,

friends or associates.

If any enquiry is received from any member of the public seeking

such details, the member of staff will politely but firmly explain the

policy to the enquirer. The member of staff will inform the enquirer

that if they wish they may leave their name address and telephone

number. This will then be passed on to the person concerned if

possible.

The member of staff will not confirm or deny whether the person

concerned is or has been a YMCA resident, member or employee

whether they have been in contact with the YMCA in any other way.

The member of staff will also explain that they will not be able to

inform the enquirer as to whether their message has been passed

on.

This procedure does not preclude disclosure of information required by statute, co-operation with such agencies as the police, social services, or probation, etc., or in a situation where life is at stake.

This procedure does not preclude disclosure of information required

by, Accountants and Auditors for the performance of their duties.

If staff were unsure of whether or not to give certain information it

should be referred to their line manager to take responsibility.

**Subject Access Requests**
Individuals have the right to make a subject access request. If an individual makes a subject access request, the organisation will tell him/her:

- whether or not his/her data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;

- to whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;

- for how long his/her personal data is stored (or how that period is decided);

- his/her rights to rectification or erasure of data, or to restrict or object to processing;

- his/her right to complain to the Information Commissioner if he/she thinks the organisation has failed to comply with his/her data protection rights; and whether or not the organisation carries out automated decision-making and the logic involved in any such decision-making.

The organisation will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless he/she agrees otherwise.

If the individual wants additional copies, the organisation will charge a fee, which will be based on the administrative cost to the organisation of providing the additional copies.

To make a subject access request, the individual should send the request to sarah.challands@sthelensymca.org.uk. In some cases, the organisation may need to ask for proof of identification before the request can be processed. The organisation will inform the individual if it needs to verify his/her identity and the documents it requires.

The organisation will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the organisation processes large amounts of the individual's data, it may respond within three months of the date the request is received. The organisation will write to the individual within one month of receiving the original request to tell him/her if this is the case.

If a subject access request is manifestly unfounded or excessive, the organisation is not obliged to comply with it. Alternatively, the organisation can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the organisation has already responded. If an individual submits a request that is unfounded or excessive, the organisation will notify him/her that this is the case and whether or not it will respond to it.

**Other Rights**
Individuals have a number of other rights in relation to their personal data. They can require the organisation to:

- rectify inaccurate data;

- stop processing or erase data that is no longer necessary for the purposes of processing;

- stop processing or erase data if the individual's interests override the organisation's legitimate grounds for processing data (where the organisation relies on its legitimate interests as a reason for processing data);

- stop processing or erase data if processing is unlawful; and

- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the organisation's legitimate grounds for processing data.

To ask the organisation to take any of these steps, the individual should send the request to sarah.challands@sthelensymca.org.uk.

**Data Security**
The organisation takes the security of personal data seriously. The organisation has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties. Computerised records are password protected and paper files are kept in locked filing cabinets with limited access.

Where the organisation engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

**Impact Assessments**
Some of the processing that the organisation carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, the organisation will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

**Data Breaches**

Members of staff are advised to be careful where they discuss

information; which could be of a private and confidential nature.

For example, such information should not be discussed on the

telephone where the member of staff might be overheard by the

public.

This includes gossiping about any subject, including one another,

particularly concerning housing, childcare management and

membership administration which may be of a private nature.

If the organisation discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The organisation will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

**International Data Transfers**
YMCA St Helens will not transfer personal data to countries outside the EEA.

**Individual Responsibilities**
Individuals are responsible for helping the organisation keep their personal data up to date. Individuals should let the organisation know if data provided to the organisation changes, for example if an individual moves house or changes his/her bank details.

Individuals may have access to the personal data of other individuals and of our customers and clients in the course of their employment, contract, volunteer period, or apprenticeship. Where this is the case, the organisation relies on individuals to help meet its data protection obligations to staff and to customers and clients.

**Individuals who have access to personal data are required:**

- to access only data that they have authority to access and only for authorised purposes;

- not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation;

- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);

- not to remove personal data, or devices containing or that can be used to access personal data, from the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and

- not to store personal data on local drives or on personal devices

that are used for work purposes.

Failing to observe these requirements may amount to a disciplinary

offence, which will be dealt with under the organisation's

disciplinary procedure. Significant or deliberate breaches of this

policy, such as accessing employee or customer data without

authorisation or a legitimate reason to do so, may constitute gross

misconduct and could lead to dismissal without notice.

**Training**

The organisation will provide training to all individuals about their

data protection responsibilities as part of the induction process and

at regular intervals thereafter.

Individuals whose roles require regular access to personal data, or

who are responsible for implementing this policy or responding to

subject access requests under this policy, will receive additional

training to help them understand their duties and how to comply

with them.

**Other Measures**

YMCA St Helens has also introduced the following measures to

further ensure compliance:

1. E-mail/Internet Access Policy has been documented to fully explain any monitoring of e-mails / internet usage.

2. CCTV Policy has been documented to fully explain the use of CCTV to ensure safety and security.

3. All ‘data controllers’ are fully trained in the procedures appropriate to data, which would include any outside Regulatory Bodies.

**Data Users Register**

YMCA St Helens is registered with the Information Commissioner’s

Office for the following purposes:

1. Staff Administration
2. Membership Administration
3. Fundraising
4. Realising the Objectives of a Charitable Organisation or Voluntary Body.
5. Accounts and Records
6. Property Management
7. Crime Prevention and Prosecution of Offenders.

**Reporting to committees**

Any complaints that have been received will be reported.

**Review and Ratification**

The policy and procedure will be reviewed by the YMCA St Helens

Board of Directors two-yearly and other committees as necessary.

Signed on behalf of YMCA St Helens

...................................................................

Richard Tully, Chairman of Board of Directors

Date: 1.5.2018

**REVIEW RECORD**

Reviewed by Housing Sub Committee 03.07.01.

Reviewed by the Board of Directors 24.07.01.

Reviewed by the Board of Directors 30.04.02.

Reviewed by the Board of Directors 27.01.2004.

Reviewed by the Board of Directors 26.07.05

Reviewed by the Board of Directors 31.07.07 – No changes

Reviewed by the Board of Directors 29.07.08

Reviewed by the Board of Directors 26.10.10

Reviewed by the Board of Directors 18.10.11

Reviewed by the Board of Directors 31.7.2012 – no changes

Reviewed by the Board of Directors 30.4.2013 – No changes

Reviewed by the Board of Directors 29.4.2014

Reviewed by the Board of Directors 28.4.2015 - No changes

Reviewed by the Board of Directors 05.5.2016

Reviewed by the Board of Directors 01.5.2018

**AMENDMENT RECORD**

**24.07.01** This Policy has been amended to take into account the current legislation.

**26.07.05** This Policy has been amended to include reference to Accountants and Auditors in 5.5

**29.07.08** Reference to Executive Director changed to Chief Executive

**26.10.10** 3.2 – Reference to the Corporation Street Training Unit deleted.4.1 – Reference to DSS changed to Benefits Agency, 4.3 – a) Reference to DHSS changed to Benefits Agency, c) Deleted. 8.1 – Reference to Executive / Deputy Chief Executive changed to Chief Executive. 9.1 – Rewritten. 10.3 – Finish sentence at job requirements, delete rest of sentence. 12.1 – Change annually to three yearly.

**18.10.11** 3.2 – Reference to recording tapes changes to recordings. 4.2 – Sports & Fitness Manager changed to HR/Activities Manager. 12 - Will be reviewed yearly, not 3 yearly. All reference to RSL deleted.

**29.4.2014** - Title Changes (HR/Activities Manager – Operational Director, Housing Manager – Housing Services Manager.

Added in reference to CCTV Policy, Named specific agencies with whom we share data.

Inclusion of Para 4 – What information is collected & held.

Moving around of information generally within the policy itself.

**5.5.2016** - Reformat to new branding including areas of work.

**1.5.2018** – Rewrite of policy and procedure to bring into line with the new GDPR.

