**Framwellgate Moor Youth And Community Association**

Reg Charity No 1154450

**Data Protection Policy (2021)**

**Data Protection Policy**

**Introduction**

We are committed to a policy of protecting the rights and privacy of individuals. We need to collect and use certain types of data in order to carry out our work of managing Framwellgate Moor Youth & Community Association (FMYCA). This personal information must be collected, stored securely, used, shared and deleted to comply with the General Data Protection Regulation (GDPR) and other relevant legislation.

The Data Protection Act (DPA 1998) and General Data Protection Regulations (GDPR 2018) govern the use of information about people (personal data). Personal data can be held on computers, laptops and mobile devices, or in a manual file, and includes email, minutes of meetings, and photographs.

The trustees, staff and volunteers are personally responsible for processing and using personal information in accordance with the Data Protection Act and GDPR. Trustees, staff and volunteers who have access to personal information will be expected to read and comply with this policy.

**Purpose**

The purpose of this policy is to set out the FMYCA commitment and procedures for protecting personal data. Trustees regard the lawful and correct treatment of personal information as essential to successful working, and to maintaining the confidence of those with whom we deal. We recognise the risks to individuals of identity theft and financial loss if personal data is lost or stolen.

The following are definitions of the terms used:

* Data Controller - the trustees who collectively decide what personal information FMYCA will hold and how it will be held or used.
* Act means the Data Protection Act 1998 and General Data Protection Regulations - the legislation that requires responsible behaviour by those using personal information.
* Data Protection Contact – the person responsible for ensuring that FMYCA follows its data protection policy and complies with the Regulations.
* Data Subject – the individual whose personal information is being held or processed by FMYCA for example a donor or hirer.
* ‘Explicit’ consent – is a freely given, specific agreement by a Data Subject to the processing of personal information about themselves. Explicit consent is needed for processing “sensitive data”, which includes:

(a) Racial or ethnic origin of the data subject

(b) Political opinions

(c) Religious beliefs or other beliefs of a similar nature

(d) Trade union membership

(e) Physical or mental health or condition

(f) Sexual orientation

(g) Criminal record

(h) Proceedings for any offence committed or alleged to have been committed

Information Commissioner’s Office (ICO) is responsible for implementing and overseeing the Data Protection Act 1998.

* Processing – means collecting, amending, handling, storing or disclosing personal information.
* Personal Information – information about living individuals that enables them to be identified – eg names, addresses, telephone numbers and email addresses. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers.

**General Data Protection Regulation (GDPR 2018)**

This contains 7 key principles for processing personal data. Personal data:

a) Shall be processed lawfully, fairly and transparently in relation to individuals,

b) Shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes,

c) Shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed,

d) Shall be accurate and, where necessary, kept up to date,

e) Shall be 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,

f) Shall be 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,

Associations are required to take responsibility for what they do with personal data and how they comply with the other principles. FMYCA must have appropriate measures and records in place to be able to demonstrate our compliance.

**Applying the Data Protection Act within the Association**

We will let people know why we are collecting their data, which is for the purpose of managing the Community Centre, its hirings, finances and compliance with the Charity Commission. It is our responsibility to ensure the data is only used for this purpose. Access to personal information will be limited to trustees, staff and volunteers.

**Correcting data**

Individuals have a right to make a Subject Access Request (SAR) to find out whether the Association holds their personal data, where, what it is used for and to have their data corrected if it is wrong, to prevent use which is causing them damage or distress, or to stop marketing information being sent to them. Any SAR must be dealt with within 30 days. Initially trustees must confirm the identity of the individual requesting a SAR before providing information, requiring both photo identification eg passport and confirmation of address eg recent utility bill, bank or credit card statement.

**Responsibilities**

Framwellgate Moor Youth & Community Association is the Data Controller under the Act and regulations, and is legally responsible for complying with Act, which means that it determines what purposes personal information held will be used for.

Trustees will take into account legal requirements and ensure that the Act is properly implemented, and will through appropriate management and strict application of criteria and controls:

a) Collect and use information fairly.

b) Specify the purposes for which information is used.

c) Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements.

d) Ensure the accuracy of information used.

e) Ensure that the rights of people about whom information is held, can be exercised under the Act.

These include:

i) The right to be informed that processing is undertaken.

ii) The right of access to one’s personal information.

iii) The right to prevent processing in certain circumstances.

iv) the right to correct, rectify, block or erase information which is regarded as being incorrect.

f) Take appropriate technical and organisational security measures to safeguard personal information.

g) Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information.

i) Set out clear procedures for responding to requests for information.

All trustees, staff and volunteers are aware that a breach of the rules and procedures identified in this policy may lead to action being taken against them.

Overall and final responsibility for general data protection regulations lies with the management committee, the Data Protection Contact on the management committee is:

Name: Peter Sykes

Contact Details: via the Centre Manager 0191 386 3356

The Data Protection Contact will be responsible for checking that the policy is implemented:

a) Everyone processing personal information understands that they are contractually responsible for following good data protection practice

b) Everyone processing personal information is appropriately informed

c) Anybody wanting to make enquiries about handling personal information knows what to do

d) Enquiries about handling personal information are dealt with promptly and courteously

f) A clear description of how the association handles personal information

g) There is a regular review and audit of the ways personal information is held and used

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the General Data Protection Regulations (2018).

In case of any queries in relation to this policy please get in touch with the Data Protection Contact.

**NOTES:**

**This Policy has been approved and authorised by**:

|  |  |
| --- | --- |
| **Name:** | Peter Sykes |
| **Position:** | Secretary |
| **Date:** | 25/03/2021 |
| **Signatures:** |  |
| **Revised:** | Policy subcommittee 25/02/2021 |
| **Reviewed & ratified:** | 25/03/2021 by Management committee (Peter Sykes) |

**Procedures for Handling Data and Data Security**

FMYCA has a duty to ensure that appropriate technical and organisational measures and training are taken to prevent:

Unauthorised or unlawful processing of personal data

Unauthorised disclosure of personal data

Accidental loss of personal data

All trustees, staff and volunteers must therefore ensure that personal data is dealt with correctly no matter how it is collected, recorded or used. This applies whether or not the information is held on paper, in a computer or recorded by some other means e.g. tablet or mobile phone.

Personal data relates to data of living individuals who can be identified from that data and the use of that data could cause an individual damage or distress. Mentioning someone’s name in a document does not comprises personal data; however, combining various data elements, such as a person’s name and salary or religious beliefs etc, would be classed as personal data, and falls within the scope of the GDPR. It is therefore important that all staff consider any information (which is not otherwise in the public domain) that can be used to identify an individual as personal data and observe the guidance given below.

**Privacy Notice and Consent Policy**

The private notice and consent policy are as follows:

Consent forms will be securely stored by the Centre Manager/Secretary in electronic or paper files.

**Operational Guidance**

**Email**:

All trustees, staff and volunteers should consider whether an email (both incoming and outgoing) will need to be kept as an official record. If the email needs to be retained it should be saved into the appropriate folder or printed and stored securely.

Remember, emails that contain personal information no longer required for operational use, should be deleted from the personal mailbox and any “deleted items” box.

**Phone Calls:**

Phone calls can lead to unauthorised use or disclosure of personal information and the following precautions should be taken:

1. Personal information should not be given out over the telephone unless you have no doubts as to the caller’s identity and the information requested is uncontroversial.
2. If you have any doubts, ask the caller to put their enquiry in writing.
3. If you receive a phone call asking for personal information to be checked/confirmed be aware that the call may come from another individual impersonating that person.

**Laptops and Portable Devices:**

All laptops/portable devices that hold data containing personal information must be protected with a suitable password.

Ensure your laptop is locked (password protected) when left unattended, even for short periods of time.

When travelling in a car, make sure the laptop is out of sight, preferably in the boot.

If you have to leave your laptop in an unattended vehicle, put it in the boot and ensure the car is locked and any alarm set.

Never leave laptops/portable devices in your vehicle overnight.

Do not leave laptops/portable devices unattended in restaurants/bars, or any public venue.

When travelling on public transport, keep devices with you at all times, do not leave them in luggage racks or even on the floor alongside you.

**Data Security and Storage:**

Store as little personal data as possible on your computer or laptop; only keep those files that are essential. Personal data received on memory stick should be saved to the relevant file on the server or laptop. The memory stick should then be returned (if applicable), safely stored or data deleted and securely disposed of.

Always password protect your computer/laptop when left unattended.

**Passwords:**

Do not use passwords that are easy to guess, they should contain a mixture of at least 6 characters, both upper and lower-case letters and numbers/symbols.

**Protect Your Password:**

Common sense rules for passwords are:

Never give out your password

Do not write your password somewhere on your laptop

Do not keep it written on something stored in the laptop case.

**Data Storage:**

Personal data will be stored securely and will only be accessible to authorised volunteers or staff.

Information will be stored for only as long as it is needed or required by statute and will be disposed of appropriately. For financial records this will be at least 6 years. Archived material such as minutes and legal documents will be stored indefinitely. Other correspondence and emails will be disposed of when no longer required or when trustees, staff or volunteers retire.

All personal data held for the association must be non-recoverable from any computer which has been passed on/sold to a third party.

**Information Regarding Employees or Former Employees:**

Information regarding an employee or a former employee, will be kept securely and indefinitely. If a situation occurs at a later time, it might be necessary to refer back to a job application or other document to check what was disclosed, in order that trustees are able to comply with their obligations (eg regarding employment law, taxation, pensions or insurance).

**Accident Book:**

This will be checked regularly. Any page which has been completed will be removed, appropriate action taken and the page filed securely.

**Data Subject Access Requests:**

We may occasionally need to share data with other agencies such as the local authority, funding bodies and other voluntary agencies in circumstances which are not in furtherance of the management of the charity. The circumstances where the law allows the association to disclose data (including sensitive data) without the data subject’s consent are:

a) Carrying out a legal duty or as authorised by the Secretary of State Protecting vital interests of a Data Subject or other person eg= child protection

b) The Data Subject has already made the information public

c) Conducting any legal proceedings, obtaining legal advice or defending any legal rights

d) Monitoring for equal opportunities purposes – ie race, disability or religion

We regard the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

We will ensure that personal information is treated lawfully and correctly.

**Risk Management:**

The consequences of breaching Data Protection/GDPR can cause harm or distress to users of the community centre if their information is released inappropriately, or they could be denied a service to which they are entitled. Trustees, staff and volunteers should be aware that they can be personally liable if they use customers’ personal data inappropriately. This policy is designed to minimise the risks and to ensure that the reputation of the association is not damaged through inappropriate or unauthorised access and sharing.