Data Protection Policy and Procedure

Document Name	Unique ID	Version	Effective Date	Review Date	Summary of significant changes
Data Protection Policy and Procedure	DPPPr	3	June 2024	June 2025	Reviewed to reflect changes from ICO in policy
Data Protection Policy and Procedure	DPPPr	3	August 2025	August 2026	Updated to include data retention timeframes and Data Use and Access Act 2025

Data Protection Policy

Purpose and Scope of Policy

Me2 Club needs to gather and use certain information about individuals. These can include:

- Children supported by Me2 Club and their families
- Volunteer
- Employees
- Trustees
- Funders
- Suppliers (including activity leaders and personnel)
- Other people the charity has a relationship with or may need to contact

This policy describes how this personal data must be collected, handled and stored to meet the Me2 Club's data protection standards and to comply with the law. This policy applies to all staff, volunteers, trustees, and third parties who process personal data on behalf of Me2 Club.

Me2 Club will register every year with the ICO. Me2 Club's registration number is **Z3604443**.

Why This Policy Exists

This Data Protection Policy ensures Me2 Club:

- Complies with the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018, the Data Use and Access Act 2025, and any other relevant legislation or guidance from the ICO
- Protects the rights of staff, children and their families, volunteers, trustees, and partners
- Is transparent about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data Protection Law

The Data Protection Act 2018 and UK GDPR describe how organisations must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or other formats.

To comply with the law, personal information must be:

- Collected and used fairly and lawfully
- Stored safely
- Not disclosed unlawfully

Data Protection Policy and Procedure

Data protection principles

The Charity is committed to processing data in accordance with its responsibilities under the GDPR. In accordance with Article 5 of the UK GDPR, personal data shall be:

a. Processed lawfully, fairly, and transparently

b. Collected for specified, explicit, and legitimate purposes

c. Adequate, relevant and limited to what is necessary

d. Accurate and kept up to date

e. Kept no longer than necessary, with retention schedules in place and secure deletion/anonymisation applied

f. Processed securely using appropriate technical or organisational measures

People, Risks and Responsibilities

This policy applies to:

- The office of Me2 Club
- All staff and volunteers
- All children and families supported by Me2 Club
- All trustees, funders, contractors, suppliers, and other individuals working on behalf of Me2 Club

Data covered includes (but is not limited to):

- Names
- Postal/email addresses
- Phone numbers
- Sensitive information (e.g. health, ethnicity, safeguarding history)

Data Protection Risks

This policy helps to protect Me2 Club from some very real data security risks, including:

- **Breaches of confidentiality**. For instance, information being given out inappropriately
- **Failing to offer choice**. For instance, all individuals should be free to choose how the Charity uses data relating to them
- **Reputational damage.** For instance, the Charity could suffer if hackers successfully gained access to sensitive data

Responsibilities

Everyone who works for or with Me2 Club has responsibility for ensuring data is collected, stored and handled appropriately. Each individual that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The **Trustees** are ultimately responsible for ensuring that Me2 Club meets its legal obligations.

- The **Chief Executive** is responsible for
    - Keeping the Trustees updated about data protection responsibilities, risks and issues. This information will usually be accessed via http://ico.org.uk, the UK's independent authority set up to uphold information rights in the public interest, promote openness by public bodies and data privacy for individuals
    - Reviewing all data protection procedures and related policies at agreed policy review dates and after any critical incident
    - Ensuring that all staff have read and understood all data protection procedures and related policies
        - On induction
        - At staff performance reviews
    - Arranging data protection training and advice for the people covered by this policy
    - Handling data protection questions from staff and anyone else covered by this policy
    - Dealing with requests from individuals to see the data Me2 Club holds about them (also called 'subject access requests')
    - Checking and approving any contracts or agreements with third parties that may handle the Charity's sensitive data
- The Trustees and Chief Executive are responsible for:
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards
    - Performing regular checks and scans to ensure security hardware and software is functioning properly
    - Evaluating any third-party services, the Charity is considering using to store or process data. For instance, cloud computing services
    - Approving any data protection statements attached to communications such as emails and letters
    - Addressing any data protection queries from journalists or media outlets such as newspapers or social media
    - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles

General Staff Guidelines

- The only people able to access data covered by this policy should be those who **need it for their work**
- **Me2 Club will provide training** to all staff to help them understand their responsibilities when handling data
- All staff should keep all data secure by taking sensible precautions and following the guidelines below
    - **Strong passwords must be used**. The outsourced IT company used by Me2 Club will be responsible for knowing all staff passwords, but would only access laptop information in an emergency or to solve a problem. PST will be responsible for knowing staff passwords in the event of long term sickness or when a member of staff leaves
    - Passwords must be changed if a member of staff leaves or if a password has been disclosed to another person thus increasing the risk of unauthorised access
    - Personal data **should not be disclosed** to unauthorised people, either within the charity or externally
    - Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of, see Data Protection Procedure Pr16
    - Staff **should request help** from their Line Manager or the Trustees if they are unsure about any aspect of data protection

Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Chief Executive or the Trustees.

When data is **stored on paper**, it should be kept in a secure place where unauthorised people cannot see or access it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a **locked drawer or filing cabinet**
- Staff should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer
- **Data printouts should be shredded** and disposed of securely when no longer needed

When data is **stored electronically** it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed as and when required. If there is a need to share a password with another member of staff (laptop sharing) once this situation is concluded the password must be changed

- If data is **stored on removable media** (like a Memory Stick, CD or DVD), they should be kept locked away securely when not being used
- Data should only be stored on **designated drives and servers** and should only be uploaded to our **approved cloud computing service Charity Log**
- Servers containing personal data should be **sited in a secure location** away from general office space
- Data should be **backed up frequently, see Data Protection Procedure below**. Those backups should be tested regularly, in line with the charity's standard backup procedures
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smartphones
- All servers and computers containing data should be protected by **approved security software and a firewall**

Data Use

Personal data is of no value to Me2 Club unless the Charity can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data staff should ensure that the **screens of their computers are always locked** when left unattended
- Personal data **should not be shared informally**. In particular, it should never be sent by email, as this form of communication is not secure
- Personal data should **never be transferred outside of the European Economic Area unless** that country or territory also ensures an adequate level of protection
- Staff **should not save copies of personal data to their own computers**. Always access and update the central copy of any data

Data Accuracy

The law requires Me2 Club to take reasonable steps to ensure data is kept accurate and up to date. All personal data is important and should be accurate, including sensitive personal data such as physical or mental health condition, racial or ethnic origin, religious beliefs, sexual orientation.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as possible**. Staff should not create any unnecessary additional data sets
- Staff should **take every opportunity to ensure data is updated**. For instance, by confirming a volunteer's details when they call
- Me2 Club will make it as **easy as possible for data subjects to update the information** Me2 Club holds about them. For instance, via the charity website

- Data should be **updated immediately if inaccuracies are discovered**. For instance, if a family can no longer be reached on their stored telephone number, it should be removed from the database

Data Retention and Deletion Schedule

Me2 Club retains personal data only for as long as necessary in line with ICO's storage limitation principle:

Children and Young People

Data Type	Retention
Child registration forms	On CRM while active, deleted 6 months after service declined
CRM records (no safeguarding)	Delete when young person turns 26 (25 + 1 year)
Records involving safeguarding	Retain **indefinitely** (minimum data only), or at least until age 26

Volunteers

Data Type	Retention
Application forms (not started)	Delete after 12 months
Active volunteer records	Retain while active
Former volunteers (non-safeguarding)	Delete after 1 year
Former volunteers (safeguarding roles)	Retain for 6 years after departure

Employees and Trustees

Data Type	Retention
Employee records	Retain for 6 years after employment ends
Trustee applications	Keep for 3 years post-departure
List of past trustees (name, term)	Retained indefinitely

Job Applicants

Data Type	Retention
Unsuccessful applications	Delete after 6 months
References (unsuccessful)	Delete after 6 months
Successful applicants	Retain for duration of employment + 6 years

Subject Access Requests

All individuals who are the subject of personal data held by Me2 Club are entitled to:

- Ask **what information** the Charity holds about them and why
- Ask **how to gain access** to it
- Be informed **how to keep it up to date**
- Be informed how the Charity is **meeting its data protection obligations**

If an individual contacts the Charity requesting this information, this is called a subject access request. Subject access requests from individuals should be made by email, addressed to the Chief Executive at [info@me2club.org.uk]. The Chief Executive can supply a standard request form, although individuals do not have to use this. Individuals will be charged £10 per subject access request. The Chief Executive will aim to provide the relevant data within 14 days. *(A response must be made within 1 calendar month of receiving the fee)*. The Chief Executive will always verify the identity of someone making a subject access request before disclosing any information.

Disclosing Data for Other Reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, Me2 Club will disclose requested data. However, the CEO or Trustees will ensure the request is legitimate, seeking assistance from the Committee or from legal advisers where necessary.

Providing Information

Me2 Club aims to ensure all individuals understand:

- What data is held
- How it is used
- How to exercise their rights

This is communicated via privacy notices and forms.

Data Protection Procedure

It is important to adhere to this procedure. It will be used for induction training and will be included in performance reviews. Before processing any personal data, all staff should consider the checklist.

Staff Checklist for recording data: -

- Do you really need to record the information?
- Is the information “standard” or is it “sensitive”?
- If it is “sensitive” do you have the data subject’s express consent?
- Has the data subject been told that this type of data will be processed?
- Are you authorised to collect/store/process the data?
    - If **'Yes'**, have you checked with the data subject that the data is accurate?
- Are you sure the data is secure?
- If you do not have the data subject’s consent to process, are you satisfied that it is in the best interests of the Me2 Club child/family, volunteer, staff or Trustee to collect and retain the data
- If recording information regarding observations, is the comment fair, accurate and justifiable?

- If I were to show this to the data subject, would I still be confident that the comment is fair, accurate and justifiable?
    - If the answer to the questions "is this comment fair, accurate and justifiable" is **'No'**, then the comment should go unrecorded
- All staff should ensure that inappropriate data is neither recorded nor retained. Once a data subject has requested access, the law specifies that data relating to him or her must not be 'weeded' i.e. it cannot be altered in any fashion before it is seen
- All staff have a duty to make sure that they comply with the data protection principles which are set out in Me2 Club's Data Protection Policy
- All data must be kept and disposed of safely and in accordance with this procedure
- Personal data shall not be transferred to a country or territory outside the European Economic Union unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

Hard and Soft Copies

Me2 Club Children

When Me2 Club is approached by a family a Child Registration form is completed and uploaded to the CRM system. The form is then stored in confidential waste ready to be shredded. The information may become out of date or inaccurate while the child is on the waiting list. When a child is taken off the waiting list the details must be checked with the family and if necessary a new form must be completed. All Forms relating to the child will be stored on the CRM system whilst the child is part of Me2 Club. Families complete their GDPR preferences on the Child Registration form which is recorded in the CRM and adhered to by Me2 Club Staff and Trustees.

The information from the Child Registration form is added to the CRM system, regular contact with see waiting list policy and when we start working with the child and their family we ensure the information is kept up to date. If, when phoning to offer a child or young person a place, you are advised that Me2 Club is no longer required, retain the form for 6 months and then destroy it by shredding.

All **child profiles** must be named with initials only and must be stored on the Office drive with password protection. All staff must ensure any information sent electronically is password protected and the password sent via another media. Once a young person turns 26, all information relating to that young person should be shredded and soft copies deleted. Where Me2 Club is aware of social care involvement (safeguarding) data relating to children/young people will be kept indefinitely. The data must be reviewed before storage to ensure only minimal information is stored, i.e. names, addresses, length of Me2 Club involvement.

Me2 Club Volunteers

All volunteers must complete an application form and references will be taken up. If the volunteer does not start working with Me2 Club within a year all documentation must be destroyed by shredding. Forms for volunteers who have left Me2 Club should be kept for 1 year and then destroyed by shredding. Sign up forms of non-trained volunteer's names should be retained in a locked cabinet for 3 months and then destroyed.

Job Applications

When candidates are required to complete an application form and the forms are sent to Trustees, they must be password protected. Trustees will delete all information relating to candidates once the role is filled. If not chosen for an interview, the form should be kept for 6 months in a safe environment and then shredded. If offered the role, references will be taken. If the applicant is unsuccessful the form/references should be kept for 6 months in a safe environment and then shredded.

Forms are kept for applicants who are successful and commence work with Me2 Club. These forms are scanned in and stored on the 'Manager' drive. If an employee leaves the information will be deleted after 6 months.

Trustees

Prospective committee members fill in a Trustee Application form. References are taken up and the person has a 3-month probationary period. If not voted onto the Committee, the forms should be kept for 6 months and then shredded.
If voted onto the Committee, the form should be kept in a safe environment for three years after the Committee member has left the Committee.
A list of all past Trustees with brief information, name, address, telephone number, is to be kept on the computer indefinitely.

Staff

All written information on a member of staff from job application form onwards should be scanned and kept on the 'Managers' drive. All hard copies will be deleted. When an employee leaves, this information will be kept for 6 years. At induction, staff will be given access to the Me2 Club Policies and Procedures. All staff have a responsibility to ensure they have read and understood them.

Trustee/Staff Meeting Minutes

Electronic copies of all Trustee/staff meetings will be kept for 6 years plus the current year.
The accounting records we must keep include:

- Accounts spreadsheet
- Invoices
- Receipts
- Annual Reports

- Financial reports submitted to Companies House
- Reports from the Independent Examiner

DBS

DBS online forms are completed by all staff, volunteers and Committee members. DBS checks are done via an online service - uCheck. Once processed, the DBS number is added onto each staff/volunteers/Trustees application form and the appropriate computer file along with the date.

Laptops

If taken out of the Me2 Club office laptops must:

- Be kept in a safe and secure environment
- Never be left unattended in any public place
- Be password protected

Server and Desktops

All desktops must be password protected and if left unattended must always be set to 'sleep' mode. All soft copy information is stored on the Me2 Club server. The sever is encrypted and password protected for extra security protection. The server is kept in a secure locked office. Me2 Club employs the services of PST Business Solutions to maintain security for Me2 Club IT equipment; as part of this support they have remote access to the server. Remote access can be gained to Me2 Club network drives via a program called 'Datto Drive'. Access is password protected.

Database

Me2 Club uses Charity Log a Client Relationship Management system (CRM) to retain information regarding children and volunteers. This CRM is double password protected and stored on the Cloud. Access cannot be gained remotely and is only available via the Me2 Club office desktops.

Phones

- Photo's should not be stored on mobile phones once uploaded to the Office drive
- Phones should be password protected

Emails

Any email of a confidential nature will be marked 'confidential' in the subject title. If writing to an unknown person there should be no recognisable reference to a Me2 Club child. Me2 Club Trustees and employees can gain access to their Me2 Club emails accounts via a password. Trustees using personal email addresses will be responsible for deleting all sensitive data.

Social Media

Data Protection Policy and Procedure

All Me2 Club employees to be aware of data protection rights of individuals whilst using social media and must NOT:

- Give confidential information about an individual
- Post a photo if permission has not been granted

Back Ups

Back-ups are done throughout the day. Data will be stored for 1 month before deletion. Monthly Office 365 backups are carried out and managed by RAD Group.

Virus Software

Me2 Club protects all desktops and laptops using anti-virus software which completes a full scan every month, daily quick scans and continual rootkit scans.

Information Commissioners Office (ICO)

It is the responsibility of the Chief Executive to ensure that Me2 Club is registered annually with the ICO.

Data Protection Declaration

Staff and Trustees will be asked to complete a Data Protection Declaration (DPD) on leaving Me2 Club.

Contact Information

Queries and Complaints: Any queries or complaints regarding data protection should be directed to the Data Protection Officer:

Data Protection Officer
Me2 Club
Reading Hockey Club
Sonning Lane
Reading
RG4 6ST

Or send an email to info@me2club.org.uk

Monitoring and Review

This policy will be reviewed annually or in response to changes in legislation or significant organizational changes. Regular audits and checks will be conducted to ensure compliance with this.