Equipping for Life

GDPR Policy

Contents

1. Context and overview

1.1 Introduction

Equipping for Life needs to gather and use certain information about individuals.

These are principally Staff, Trustees, Donors and Volunteers - but can include other customers, suppliers, business contacts, employees and other people the organisation 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 company's data protection standards - and to comply with current data protection law.

1.2 Why this policy exists

This data protection policy assists Equipping for Life to take all reasonable steps to:

- comply with data protection law and follow good practice;
- protect the rights of staff, customers and business partners;
- be open about how it stores and processes individuals' data; and
- protect itself from the risks of a data breach.

1.3 Data protection law

The Data Protection Act 2018 and the EU General Data Protection Regulation describes how organisations such as Equipping for Life must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly, lawfully and transparently;
- used for specified, explicit purposes;
- used in a way that is adequate, relevant and limited to only what is necessary;
- accurate and, where necessary, kept up to date;
- kept for no longer than is necessary; and
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

2. People, risks and responsibilities

2.1 Policy scope

This policy applies to:

- the Office Manager of Equipping for Life;
- all branches of Equipping for Life;
- all staff and volunteers of Equipping for Life; and
- all contractors, suppliers and other people working on behalf of Equipping for Life.

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 2018. This can include:

- names of individuals;
- postal addresses;
- email addresses;
- telephone numbers; and
- any other information relating to individuals

2.2 Data protection risks

This policy helps to protect Equipping for Life from some significant security risks which are included in the list below.

- 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 company uses data relating to them. Where for example Schools, but also other organisations that can reasonably be said to be *in loco parentis,* transmit bulk lists of users, Equipping for Life will treat such bulk data exchange as if it were from an individual.
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

2.3 Responsibilities

Everyone who works for or with (such as volunteers) Equipping for Life has some responsibility for ensuring data is collected, stored and handled appropriately and in accordance with this Policy.

Each person who handles personal data must ensure that it is handled and processed in line with this Policy and data protection principles.

The key areas of responsibilities associated with individuals and groups are listed below.

• The Board of Trustees is ultimately responsible for ensuring that Equipping for Life meets its legal obligations.

• The Data Protection Officer, Dr Darrin Barr, is responsible for:

- keeping the Board updated about data protection responsibilities, risks and issues;
- reviewing all data protection procedures and related policies, in line with an agreed schedule;
- 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 Equipping for Life holds about them (also called 'subject access requests');
- reporting data breaches to Information Commissioner's Office (if required); and
- checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

• Mrs Pat Hutchinson, Company Secretary, is 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; and
- evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

• The Director, Ms Audrey Curry, is responsible for:

- addressing any data protection queries from journalists or media outlets like newspapers;
- implementing the Data Breach Management Procedure; and
- where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

• The Board of Trustees is responsible for:

- approving GDPR related policies and procedures;
- approving any data protection statements attached to communications such as emails and letters; and
- ensuring compliance with the policies and procedures.

3. General guidelines for staff

- The only people able to access data covered by this policy should be those who need it for their work
- Data should not be shared informally. When access to confidential information is required, employees can request it from their managers.
- Equipping for Life will provide training to all employees on induction and at regular intervals as appropriate to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking reasonable precautions and following the guidelines set out below.
- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the company 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.
- Employees should request help form the Data Protection Officer if they are unsure about any aspect of data protection.

4. Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Secretary.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see 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.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, such as on a printer.
- Data printouts should be shredded and disposed of securely when no longer required

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 and never shared between employees.
- If data is stored on removable media (like a CD or DVD), these 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 an approved cloud computing service
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should never be saved directly to mobile devices such as smartphones. Other laptops and tablets must have suitable protection measures such as file and folder encryption deployed.
- All servers and computers containing data should be protected by approved security software and a firewall.

5. Data use

In the normal course of business Equipping for Life makes appropriate use personal data. However, it is when personal data is received, accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure 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 other than the company's email service and for official company business only.
- Data must be encrypted before being transferred electronically. The Secretary can explain how to send data to authorised external contacts.
- Personal data should never be transferred outside of the European Economic Area.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

6. Data accuracy

The law requires Equipping for Life to take reasonable steps to ensure data is accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Equipping for Life should put into ensuring its accuracy.

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 necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated as appropriate for operations. For instance, by confirming a customer's details when they call.
- Equipping for Life will make it easy for data subjects to update the information the Company holds about them.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored email, it should be removed from the database, with an appropriate comment.
- It is the Director's responsibility to ensure marketing databases are kept up to date, and comply with this policy.

7. Subject access requests

All individuals who are the subject of personal data held by Equipping for Life are entitled to:

- Ask what information the company 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 company is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a "subject access request".

Subject Access Requests from individuals should be made by email, addressed to the data controller at pat@equippingForLife.org.uk . The Data Protection Officer can supply a standard request form, although individuals do not have to use this provided they supply sufficient information to enable the Company to identify the relevant record.

Individuals will be charged £10 per subject access request. The Data Protection Officer will aim to provide the relevant data within 10 working days of receipt.

The Data Protection Officer will always verify the identity of anyone making a Subject Access Request before handing over any information.

8. 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, Equipping for Life shall disclose the requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the Board and/ or from the company's legal advisers where necessary.

9. Providing information

Equipping for Life aims to ensure that individuals are aware that their data is being processed and that they understand:

- how the data is being used; and
- how to exercise their rights.

To these ends, the Company has a privacy notice, setting out how data relating to individuals is used by the company. See Schedule 1.

10. Dealing with a suspected or actual data breach

See Data Breach Management Procedure (Schedule 3)

Schedule 1: Equipping for Life - Privacy Notice – March 2022

Equipping for Life is a registered charity and company limited by Guarantee. Founded by Brother David Jardine in Spring 2018, Equipping for Life enables people of faith to volunteer their time in communities that have been impacted by deprivation. We seek to equip people for a better life by our volunteers supporting existing education, employability and social cohesion initiatives.

Our Vision is: Lives transformed; communities revitalized.
Our Mission is: To equip people for a better future.
Our Values are: Faith, Integrity, Equality, Hope.

This privacy policy sets out how Equipping for Life uses and protects any information that you give to Equipping for Life when you engage with us as an Equipping for Life volunteer or Prayer Partner or Donor.

Equipping for Life is committed to ensuring that your privacy is protected. Should we ask you to provide certain information, by which you can be identified, then you can be assured that it will only be used in accordance with this privacy statement.

Equipping for Life may change this policy from time to time by updating this page. You should check this page regularly to ensure that you are happy with any changes. This policy is effective from August 2019.

1. What we collect

We may collect the following information:

- Name, address, date of birth and job title etc.
- Donor (Bank details when appropriate ie BACS transfer)
- Donor (Tax payer Gift Aid purposes)
- Other contact information including email address, home number and mobile
- Demographic information such as postcode, preferences and interests
- Other information relevant to a client survey
- Verification Documents for Access NI Checks. These will be shredded or deleted 90 days after receipt of information/certificates.

2. What we do with the information we gather

We require this information to administer your application to become a volunteer, understand your needs and provide you with a better service, process any donations and for the following reasons:

- Internal record keeping.
- We may use the information to improve our services.

- We may periodically send promotional emails about new services, events or initiatives or other information which we think you may find interesting using the email address which you have provided.
- From time to time, we may also use your information to contact you for the purposes of conducting surveys about your experience of volunteering in schools or other training organisations. We may contact you by email, phone or mail. We may also use the information to customise the website according to your interests.
- Carry out our legal duties and statutory responsibilities eg Access NI checks, where required.

3. Legal basis for collecting and using your personal data

We will only use your Personal Data if we have valid reasons for doing so. This will include

- With your consent;
- Legal obligations, where we are required to process it under law;
- Legitimate interests, where we are required to process data for business related tasks

4. Security

We are committed to ensuring that your information is secure. In order to prevent unauthorised access or disclosure, we have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information we collect online or as hard copy.

5. Who we may share your data with

We will share your information, including contact and AccessNI details, with the relevant staff in the Primary School where you are volunteering as a tutor.

In addition, your contact details only will be shared with the volunteer members of your Team at the School where you are a tutor, to assist with communication between the members.

6. Controlling your personal information

You may choose to restrict the collection or use of your personal information in the following ways:

- if you have previously agreed to us using your personal information for direct marketing purposes or agreeing to be a Prayer Partner, you may change your mind at any time by writing to or emailing us at: pat@equippingforLife.org.uk

We will not sell, distribute or lease your personal information to third parties unless we have your permission or are required by law to do so. We may use your personal information to send you promotional information about third parties which we think you may find interesting if you tell us that you wish this to happen.

You may request details of personal information which we hold about you under the Data Protection Act 2018 and the EU General Data Protection Regulation. If you would like a copy of the information held on you please write to Data Protection Office, Equipping for Life, 9c Argyle Business Centre 39 North Howard Street, Belfast BT13 2AP.

If you believe that any information we are holding on you is incorrect or incomplete, please email us: pat@equippingforLife.org.uk or write to the above address as soon as possible. We will promptly correct or delete any information found to be incorrect.

7. Additional Information

Further details are provided in our GDPR Policy which can be accessed at our Website, https://www.equippingforlife.org.uk/

8. Complaints

You have the right to complain about how we treat your Personal Data to the Information Commissioner's Office (ICO). The contact address for the ICO is:

Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF

Schedule 2: Authorised Administrators

Authorised Administrators of Equipping for Life:

Name	Date of Authorisation
1. Mrs P Hutchinson MBE	28th Jan 2019
2. Dr D Barr	31st March 2022

Schedule 3: Data Breach Management Procedure

This is an internal procedure and does not need to be published. It should be made available to all staff.

EXECUTIVE STATEMENT

Equipping for Life collects, holds, processes and shares large amounts of personal data, a valuable asset that needs to be suitably protected. Every care is taken to protect personal data and to avoid a data protection breach, however, in such circumstances, it is vital that immediate action is taken to contain and remedy the breach.

The Data Protection Officer (DPO) is legally required to notify the Information Commissioner's Office (ICO) of any personal data breach within 72 hours of becoming aware of it therefore it is essential that immediate action is taken by Equipping for Life when a breach has occurred or is likely to occur. Individuals affected by the personal data breach must also be notified promptly.

Following the containment and remedy stage, steps must be taken to assess and determine the cause of the breach to ensure processes are reviewed and risk is minimised going forward.

This Data Breach Management Procedure (the Procedure) provides guidance for staff members on how a Personal Data Breach should be handled and is intended for internal use.

It places obligations on staff to report actual or suspected personal data breaches and sets out the steps to be followed by Equipping for Life for managing and recording actual or suspected breaches. The Procedure applies to all personal data held and processed by Equipping for Life regardless of format.

1. Scope

1.1 The aim of this Procedure is to standardise the response to all reported data breach incidents, and ensure that they are appropriately logged and managed in accordance with best practice guidelines.

1.2 By adopting a standardised, consistent approach to all reported incidents it aims to ensure that:

1.2.1 immediate action is taken;

1.2.2 incidents are handled by appropriately authorised and skilled personnel;

1.2.3 incidents are recorded and documented;

1.2.4 the impact of the incidents are understood and action is taken to prevent further damage;

1.2.5 external bodies or Data Subjects (defined below) are informed as required;

1.2.6 incidents are dealt with in a timely manner and normal operations restored;

1.2.7 evidence is gathered, recorded and maintained in a form that will withstand internal and external scrutiny; and

1.2.8 incidents are reviewed to identify improvements in policies and procedures.

1.3 **The following terminology is used in this Procedure:**

Term	Meaning
Data Protection Officer or DPO	The person we appoint from time to time to be involved in all aspects of the development and implementation of our data protection and data privacy strategy and compliance with the GDPR and other applicable laws.
Data Subject	The individual to whom the personal data relates.
GDPR	The General Data Protection Regulation.
Personal Data	Information relating to an individual who can be identified (directly or indirectly) from that information.
Personal Data Breach	Any incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed, e.g. accidental loss, destruction, theft, corruption or unauthorised disclosure of Personal Data.
Special Category Data	Personal Data about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetic information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

2. What is a Personal Data Breach?

2.1 A Personal Data Breach causes, or has the potential to cause, damage to Equipping for Life's information assets, its reputation or to a Data Subject. A personal data breach may be recent, or historical and only just discovered.

2.2 Examples of a Personal Data Breach include but are not restricted to, the following:

2.2.1 loss or theft of Personal Data or equipment on which Personal Data is stored (e.g. loss of laptop, USB pen, iPad/tablet device, hard copy file or paper record);

2.2.2 alteration of personal data without permission or authorisation;

2.2.3 unauthorised disclosure of Personal Data;

2.2.4 sending Personal Data to the wrong recipient;

2.2.5 attempts (failed or successful) to gain unauthorised access to information or IT systems;

2.2.6 loss of availability of Personal Data (e.g. hacking attacks);

2.2.7 'blagging' offences where information is obtained by deceiving the organisation who holds it;

2.2.8 human error;

2.2.9 an identified vulnerability or weakness which may lead to a Personal Data breach.

3. Who is responsible under this Procedure?

3.1 All staff, workers, contractors or volunteers employed or otherwise engaged at Equipping for Life must report any actual, suspected, threatened or potential Personal Data Breach and assist with investigations as required, particularly if urgent action is required to prevent further damage.

3.2 Staff are responsible for overseeing the implementation of recommendations resulting from a Personal Data Breach so far as possible within their control.

3.3 The Director must ensure that all staff, workers, contractors and volunteers comply with this Procedure, assist with investigations and implement improvement measures. The Director is also the primary point of contact within Equipping for Life for any data protection issues and is the interface with Equipping for Life's DPO. The Director will work closely with the DPO in relation to any actual, suspected, threatened or potential Personal Data Breach.

The Data Protection Officer (DPO) is responsible for supporting the Director in managing a Personal Data Breach in accordance with this Procedure and will be the point of contact with the ICO. In our case, the Education Authority is our DPO and contact details are as follows:
Email: darrin@equippingforlife.org.uk

4. Reporting a Personal Data Breach

4.1 Anyone discovering an actual, suspected, threatened or potential Personal Data Breach must report it immediately to the Director as the primary point of contact.

4.2 The Director must then immediately, and in any event within one hour, report the Personal Data Breach to the DPO using the Data Breach Report Form set out in Appendix 1.

4.3 Any actual, suspected, threatened or potential Personal Data Breach discovered outside of normal working hours must be reported by contacting the Director (email audrey@equippingforlife.org.uk).

4.4 The Director's report to the DPO should include full and accurate details of the incident including who is reporting the incident and what Personal Data is involved.

4.5 When a data breach has been reported to the DPO, the incident will be logged on a central system to facilitate effective management of the breach and to aid reporting.

4.6 All staff should be aware that any Personal Data Breach by them or any failure to report a Personal Data Breach in accordance with this paragraph 4 may result in the matter being considered under the relevant disciplinary procedure.

5. Dealing with a Personal Data Breach

5.1 There is no single method of response to a Personal Data Breach. Incidents must be dealt with on a case by case basis.

5.2 <u>Evaluate the severity of the Personal Data Breach</u>

5.2.1 Once a Personal Data Breach has been reported to the DPO, an initial assessment will be carried out by the DPO in conjunction with the Director to establish the severity of the incident.

5.2.2 The DPO and the Director will evaluate the severity of the Personal Data Breach by considering the following factors:

(a) the impact to the individuals concerned

- this is the overriding consideration in deciding whether a Personal Data Breach should be reported to the ICO.
- impact includes emotional distress as well as both physical and financial damage. It can include:
    - exposure to identity theft through the release of non-public identifiers, e.g. passport number
    - information about the private aspects of a person's life becoming known to others, e.g. health or medical conditions.

(b) the sensitivity of the Personal Data

- there should be a presumption to report to the ICO where smaller amounts of Personal Data are involved, the release of which could cause a significant risk of individuals suffering substantial detriment, including substantial distress.
- this is most likely to be the case where the Personal Data Breach involves Special Category Personal Data. If the information is particularly sensitive, even a single record could trigger a report.

(c) the volume of Personal Data involved

- there should be a presumption to report to the ICO where:
  - a large volume of personal data is concerned, and
  - there is a real risk of individuals suffering some harm.
- it will, however, be appropriate to report much lower volumes in some circumstances where the risk is particularly high, e.g. because of the circumstances of the loss or the extent of information about each individual.

(d) the number of individuals concerned.

(e) the potential media interest.

(f) the impact on Equipping for Life.

5.2.3 Specific consideration will be given to whether Data Subjects will suffer any discrimination, identity fraud, financial loss, reputational damage, loss of confidentiality and economic or social disadvantage, as a result of the Personal Data Breach.

5.3 **Containment and Recovery**

5.3.1 The Director, supported by the DPO, will take appropriate steps as necessary to contain the Personal Data Breach and recover the Personal Data as quickly as possible. Such steps will include (but are not limited to):

(a) immediately contain the Personal Data Breach (if this has not already occurred). Corrective action may include retrieval or recovery of the Personal Data, ceasing unauthorised access, shutting down or isolating the affected system;

(b) where the Personal Data Breach relates to a centrally managed ICT system, notify IT Consultant immediately (as required);

(c) contact relevant staff to advise of precautionary measures where a risk remains live (as required);

(d) utilise expertise of staff within Equipping for Life, and external contractors as appropriate;

(e) attempt to retrieve misdirected emails and contact recipients to instruct them to delete and destroy the material sent to them in error;

(f) ensure that any codes or passwords are changed where the information has been compromised and that users are notified;

(g) assess the availability of back-ups where Personal Data is damaged/lost/stolen;

(h) whether there are wider consequences to the Personal Data Breach.

5.4 **Notifications/Communications**

Notification to Information Commissioner's Office

5.4.1 The DPO and the Director will establish whether the Personal Data Breach needs to be reported to the ICO. Where the decision is taken to notify the ICO, the DPO will report the Personal Data Breach within 72 hours of the Personal Data Breach being initially discovered.

5.4.2 A decision to report or not to report the Personal Data Breach will be based on an assessment of the severity of the Personal Data Breach and any potential risk to the rights and freedoms of the Data Subjects. The ICO's 'Self Assessment of a Data Breach Tool' can be used to assess if the data breach should be reported.

5.4.3 Where a Personal Data Breach is reported to the ICO, the following information must be included within the report:

(a) a description of the of the Personal Data Breach;

(b) the categories and approximate number of individuals concerned;

(c) the categories and approximate number of Personal Data records concerned;

(d) the name and contact details of the DPO and where more information can be obtained;

(e) description of the likely consequences of the Personal Data breach; and

(f) a description of the measures taken, or proposed to be taken, to deal with the Personal Data Breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

5.4.4 ICO contact details are available at **https://ico.org.uk/for-organisations/report-a-breach/.**

Notification to Data Subjects

5.4.5 The Director and the DPO will consider the need to notify the Data Subjects. This decision will be based on the risk to the rights and freedoms of Data Subjects. The Director will notify the affected Data Subject(s) without undue delay, including:

(a) full details of the Personal Data Breach including a description of the Personal Data affected;

(b) the likely consequences of the Personal Data Breach;

(c) the measures we have or intend to take to address the Personal Data Breach, including, where appropriate, recommendations for mitigating potential adverse effects; and

(d) a name and contact point within Equipping for Life.

5.4.6 When determining whether and how to notify Data Subjects of the Personal Data Breach, Equipping for Life will:

(a) co-operate closely with the ICO and other relevant authorities, e.g. the police; and

*(b) take account of the factors set out in **Appendix 2**.*

Notification to the Police

5.4.7 The Director, supported by the DPO, will consider the need to contact the police for the purpose of containment and recovery. In addition, where it transpires that the Personal Data Breach arose from a criminal act perpetrated against Equipping for Life, Equipping for Life will notify the police and/or relevant law enforcement authorities.

Notifying Other Parties

5.4.8 The Director, supported by the DPO, will consider whether there are any legal or contractual requirements to notify any other parties.

5.5 Evaluation and Response

5.5.1 Once the incident is contained, the Director will lead a full review of:

(a) the cause(s) of the Personal Data Breach;

(b) the effectiveness of the response(s); and

(c) whether any changes to the systems, policies and procedures should be undertaken.

5.5.2 All staff, workers, contractors or volunteers employed or otherwise engaged at Equipping for Life will be required to comply in full and promptly with any investigation.

5.5.3 An audit will be led by the Director within 6 months from the date of report to ensure that recommendations have been implemented.

Schedule 3 APPENDIX 1

Data Breach Report Form	
Time and Date Personal Data Breach was identified **(Also time and date breach occurred if different to when identified)**	
Who is reporting the breach: Name/Post/Dept	
Contact details: **Telephone/Email**	
Description of the Personal Data Breach:	
Volume of Personal Data involved and number of individuals affected	
Is the breach confirmed/suspected/ **possible/threatened?**	
Is the breach contained or ongoing?	
What actions are being taken **to stop the breach and/or recover the data?**	
Who has been informed of the breach?	
Any other relevant information	

Email form to audrey@equippingforlife.org.uk and darrin@equippingforlife.org.uk

Received by:	
Date/Time:	

Schedule 3 APPENDIX 2

FACTORS AFFECTING IF AND HOW TO NOTIFY DATA SUBJECTS OF A PERSONAL DATA BREACH

Factor	Impact on obligation to notify data subject
Whether we have implemented and applied (to the affected personal data) appropriate technical and organisational protection measures—in particular measures that render the personal data unintelligible to any person who is not authorised to access it, e.g. encryption.	Where such measures have been implemented, it is not necessary to notify the data subject(s).
Whether we have taken measures following the personal data breach which ensure the high risk to the rights and freedoms of data subjects affected by that breach is no longer likely to materialise.	Where such measures have been implemented, it is not necessary to notify the data subject(s).
Whether it would involve disproportionate effort to notify the data subject(s).	If so, it is not necessary to notify the data subject(s)—but we must, instead, issue a public communication or similar measure whereby the data subjects are informed in an equally effective manner.
Whether there are any legal or contractual requirements to notify the data subject?	If yes, it may be necessary to notify the data subject(s) in any event.

Schedule 4: ***Disposal of Records Schedule***

1. Purpose of Disposal Schedule

This disposal schedule identifies the disposal arrangements for all manual and electronic records created by Equipping for Life. The Schedule complies with the requirements of the Public Records Act (NI) 1923 and the Disposal of Documents Order (S.R.& O.1925 No 167).

2. Categories of Disposal

- Destruction
- Permanent preservation

3. Operation of this Records Disposal Schedule

a. Closing a File

Manual records should be closed as soon as they cease to be of active use other than for reference purposes. When a file is due to be closed an appropriate member of staff should consult the disposal schedule and mark the front cover of the file, indicating the date on which the file can be destroyed, or whether it should be reviewed by a member of staff. Closing a file simply means that no further papers can be added but the file can be used for reference.

b. Minimum Retention Period

The minimum retention period required for each type of record is calculated from the point the file/record is closed.

c. Destroy

Where the disposal action states 'Destroy' the records should be kept for the period stated and then destroyed securely. A record must be maintained of the files that have been destroyed.

d. Commitment to preserving files/records

EfL declares that it will take measures to ensure that the records it creates (including electronic records) will be well maintained and protected while they are in its custody.

e. Roles and Responsibilities

The Board of Trustees is responsible for ensuring that EfL complies with the commitment laid out in this Schedule. The Director is charged with operational compliance and will assign any specific staff responsibilities as required in order to help fulfil EfL's commitment to effective

records management. All members of staff are responsible for creating and maintaining records in accordance with good records management practice.

4. Definitions of Records held.

There are six main functional areas for which Equipping for Life keeps records as follows:

I. Management and Organisation

II. Legislation & Guidance

III. Staff

IV. Volunteers

V. Finance

VI. Health & Safety

5. Electronic Records

The legal obligation to properly manage records, including compliance with GDPR legislation, applies equally to electronic records. The main considerations for the management of electronic records are therefore the same as those for manual records. They include:

- Staff must be able to use and access electronic information effectively
- Adequate measures must be in place to ensure all information is stored securely and only available to authorised persons.
- EfL must be able to demonstrate a record's authenticity by ensuring information cannot be altered when declared a record.
- A system must be in place for disposing of electronic records in line with policy once they are no longer needed.

In addition to the above, sufficient backup/recovery processes must be in place. There must also be a process through which links are created from electronic records to any associated manual records. This is to ensure a full record can be considered when necessary i.e. when decision making, providing access or considering a record for disposal.

Record Disposal Schedule

1. Management & Organisation

Ref	Record	Minimum Retention Period	Action After Retention
1.1	Board of Trustees – general correspondence	Current year + 6 years	Destroy
1.2	Board Meetings Minutes (master)	Current year + 6 years	
1.3	Senior Management Team-Meeting Minutes	Current year + 6 years	
1.4	Policies	Retain while current. Retain 1 copy of old policy for 2 years after being replaced	Destroy
1.5	Comments/Complaints	5 years after closing. Review for further retention in the case of contentious disputes	Destroy
1.6	Emergency Planning/Business Continuity Plan	Until superseded	Destroy

2. Legislation and Guidance from Charities Commission, HMRC, HSENI etc

Ref	Record	Minimum Retention Period	Action After Retention
2.1	Circulars, Guidance, Bulletins, Letters etc	Until superseded	Destroy

3. Staff

Ref	Record	Minimum Retention Period	Action After Retention
3.1	Staff Personnel Records (including, appointment details, training, staff development etc.)	7 years after leaving employment	Destroy
3.2	Interview notes and recruitment records	Date of interview + 6 years	Destroy
3.3	Staff Salary Records	7 years after leaving employment	Destroy
3.4	Staff Sickness Records (copies of Medical Certs)	Current year + 6 years	Destroy
3.5	Procedures for Induction of Staff	Until superseded	Destroy
3.6	Staff Attendance Records	7 years after leaving	Destroy

4. Volunteers

Ref	Record	Minimum Retention Period	Action After Retention
4.1	AccessNI Information	90 days (with exceptions)	Destroy
4.2	Interview notes	Date of interview + 6 years (or when they leave, unless permission is granted from Volunteer to retain)	Destroy
4.3	Contact Details	7 years after stopping volunteering	Destroy
4.4	Training Records	Current year + 6 years	Destroy

5. Finance

Ref	Record	Minimum Retention Period	Action After Retention
4.1	Annual budget and budget deployment	Current financial year + 6 years	Destroy
4.2	Budget Monitoring	Current financial year + 6 years	Destroy
4.3	Annual Statement of Accounts	Current financial year + 6 years	Destroy
4.4	Order Books, Invoices, Bank Records, Cash Books, Till Rolls, Lodgement books etc	Current financial year + 6 years	Destroy
4.5	Postage Book	Current financial year + 6 years	Destroy
5.6	Company Accounts	Current financial year + 6 years	Destroy

6. Health & Safety

Ref	Record	Minimum Retention Period	Action After Retention
5.1	Accident Reporting	Date of incident + 7 years	Destroy
5.3	Risk Assessments	7 years	Destroy
5.4	H & S Reports	15 years	Destroy
5.5	Fire Procedure	Until superseded	Destroy
5.6	Security System File	For the life of the system	Destroy

Policy Review	
Date & Type of Review	**Date Approved by Board**
April 2022, minor changes, addition of Data Breach Management Procedure & Disposal of Records Policy	10/05/22