

GDPR Annual Report

Submission Date: 28th November 2022

Submitted By: Caryn Nicolson

Submitted To: Board of Trustees

-
1. Purpose of the Report: To update on GDPR compliance progress within the 2021/22 operational year.
 2. About the Reporting Requirement: Organisations are required to report annually on GDPR compliance in accordance with the new Data Protection Act 2018.
 3. Responsible Person(s): Natasha Johnstone, Data Protection Officer.
 4. Reporting Period: 1st April 2021 – 31st March 2022.
 5. Reporting / Notification

Based upon our notification register the following were reported for the year.

- Subject Access Requests – None
- Requests for the Erase of Data – None
- Data Breaches – One

Notification

Having reviewed the data breach (as noted in item 5 above) using the ICO's assessment tool and having sought advice, this breach did not register as notifiable, therefore no formal notifications to the ICO were submitted for the year. For the purposes of organisational performance reporting, notifications are reported to the Board on a quarterly basis.

6. Summary of Policies/Procedures in Place:

Since October 2018, the charity has had in place the following policies.

- Safeguarding policy and procedure and framework
- Using, Managing and Protection Personal Data

For operational management purposes, each year improvement objectives are identified and acted upon unless some substantial reason is given not to do so or prohibits, or delays action being taken.

The actions planned from the previous year for this year are as follows

- Creation of Internet Policy
- Carry out an Annual Audit
- Carry out Ongoing Training

Summary 4 Year Action Plan

Year One (2019)	Year Two (2020)	Year Three (2021)	Year Four (2022)
Train Board of Trustees (Completed)	Implement GDPR Compliant Framework for each service: Privacy Notice, Consent Forms, Form of authority, article 30 documentation, legitimate interest assessments. (Completed)	Train any staff members who have not had GDPR training. (Ongoing)	Update of Internet Policy (Outstanding)
Train All Staff (Completed)	Data Protection Templates (Completed)	Create a training timetable to ensure staff received refresher training after 2 years. (Completed)	Carry out an annual audit. (Outstanding)
Data Mapping (Completed)	Data storage and retention schedule (Completed)	Complete the Implementation of GDPR Compliant Framework for Admin department (On Hold)	Reduction of client data stored on SharePoint (Ongoing)
Desktop Audit with all client facing staff (Completed)	Update Client Guide (Completed)	Destroy data which does not comply with the data and storage retention schedule.	Creation and Implementation of GDPR fundraising paperwork (Outstanding)

		(Completed and ongoing)	
Review of Partner Contracts	Update Partner agreements.	Upload of Privacy notice on FLF website	
	Training off all new staff during induction. (On going)	Implement GDPR complaint recruitment / personal paperwork. (Completed)	

7. Actions Taken within the Year:

- Electronic & paper data (held in our lockup) was destroyed in line with retention schedule.
- Mobile Phone and Sharepoint access security upgrade to Double Authentication
- Ongoing Training

FLF was unable to take forward its planned activity for the year due to a change in management, the impact of Covid 19 and work demands which were unplanned. As a result, we could not take forward all planned actions as noted in item 6 of this report. Outstanding planned work will be reassessed in the forthcoming year.

8. Recommendations/Concluding Statements:

As a result of changes to FLF's management structure and the need to respond to service delivery redesign, planned work for this and other requirements were reprioritised in relation to capacity and risk. Having undertaken a review, improving the security of systems was determined as a priority action for the year and therefore, this was a key focus of activity for the year. The following recommendations are made for the forthcoming year.

- It is recommended that the administration of GDPR and policies are reviewed to determine proportionate activity in relation to current resources.
- It is recommended that staff continue to receive training during their first year of employment and retraining takes place every 2 years.
- An annual audit of one service should be carried out to ensure practice remains robust.