The CIFA Trust

Data Protection Policy

Contents

1. Summary

1.1 This policy will be reviewed bi-annually to ensure it is up to date. If significant changes to government policy or guidance occur, this policy should be reviewed as appropriate.

1.2 This policy will set out how the organisation will handle the data it holds on service users. The document provides guidance based on the data protection principles and obligations as contained in the GDPR and as supplemented by the UK Data Protection Act 2018. Their content is relevant to all trustees and any volunteers or staff throughout the organisation.

1.3 The intended outcome of this data protection policy document is that the organisation obtains, stores, uses, discloses and disposes of personal data about living individuals in line with legislative requirements, no matter how that information is held.

2. Scope

2.1 Data protection law has undergone significant changes in recent times. The EU General Data Protection Regulation 2016/679 (GDPR) came into force on 25 May 2018 and had direct effect in all EU Member States from that date onwards, without the need for any national legislation. The GDPR is supplemented by the UK Data Protection Act 2018.

2.2 The GDPR defines 'personal data' and 'special categories of personal data'. The definitions can be located on the ICO website at the links below:

- Personal data - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/
- Special category data - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/

3. Trustee Responsibilities

3.1 Trustees are required to familiarise themselves with the content of the data protection and subject access policy and to be aware of the associated procedure and guidance documents.

The responsibility for having detailed knowledge of the procedure and guidance, cascading this to any volunteers or staff, and the monitoring of compliance to these documents within the organisation may be carried out by a nominated member of the board or delegated by them to an appropriate member of any management team.

4. Legislation

4.1 The organisation will seek to comply with the GDPR in the way it collects, processes, maintains, stores and disposes of data, ensuring it is:

- processed lawfully, fairly, and in a transparent manner;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary for the purpose for which the data is processed;
- accurate and where necessary kept up to date;
- not kept for longer than is absolutely necessary for its given purpose; and
- subject to appropriate security to safeguard against unauthorised or unlawful use, destruction or damage.

The organisation is also required to demonstrate how it is complying with its obligations under the GDPR, by ensuring that appropriate systems, controls and procedures are in place.

4.2 The organisation is required to nominate a Data Protection Officer (DPO). The DPO must be selected on the basis of professional qualities and expert knowledge of data protection law but does not need to be legally qualified. In particular, the DPO must:

- be informed of all data protection issues within the organisation in a proper and timely manner;
- be provided with the necessary resources to carry out their tasks and have access to all personal data operations;
- have autonomy to undertake their tasks; and
- report to the highest level of management and not be dismissed or penalised for performing their tasks.

5. Rights of Data Subject

5.1 Where personal information is kept, the individual to whom it applies has the right to access it and (amongst other rights) is entitled to correct any error or omission.

6. Data Security breaches

6.1 Everyone has a right to expect their personal data to be held and handled securely and confidentially. The organisation is required to have safe, effective systems in place to deal with breaches of security swiftly and effectively.

6.2 In the event of a data breach, a data breach form must be completed, latest guidance from the Information Commissioners Office (ICO) reviewed and if appropriate must be reported to ICO within 72 hours.

7. Archiving and Destruction

7.1 The organisation will not keep personal or sensitive data for longer than necessary to fulfil the purpose for which it is held and will have systems in place to ensure its safe archiving and destruction.

8. Review and adoption

8.1 The organisation's Board of Trustees is required to formally adopt this policy and to ensure a documented record is kept of their decision to do so.

8.2 Details of the policy (namely its title and any reference number) and the date it was adopted will be documented in the minutes of the appropriate trustee board meeting as evidence of the decision taken. The minutes will be signed by the chair of the trustees on behalf of the board.