DATA PROTECTION POLICY

Document Control	
Approved By:	AmplifyChange Directors
Responsible Owner:	Operations Manager
Created:	June 2021
Revised:	24 April 2024 (see revision schedule at end)
Approved:	
Next Review:	April 2025
Version	2

Table of Contents

Photo credit: Nifin'Akanga

1. Introduction and scope

AmplifyChange may collect and hold personal data about its staff, consultants, directors and members, grantees, donors, event attendees, and other individuals who work with or contact the organisation. AmplifyChange is committed to ensuring that this personal information is managed responsibly and in accordance with data protection legislation, other related policies and any associated legislation or Codes of Practice.

This policy covers all personal information held by AmplifyChange including that contained in its own records and that held in its physical and digital archives and deposited collections.

All AmplifyChange staff, contractors, directors and members are required to ensure that they comply fully with this policy and its associated procedures.

A full list of associated policies and procedures can be found in the Appendix.

2. The legislation

AmplifyChange is subject to the following laws in regard to personal data:

- **The UK General Data Protection Regulation (UK GDPR)** - sets out the data protection principles and legal basis for processing, the rights of data subjects, the obligations of data controllers and processors, international transfers, and enforcement
- **The Data Protection Act 2018 (DPA 2018)** - sets out the data protection framework for UK data protection law, defining exemptions and the powers of Information Commissioner's Office (ICO), the UK's regulator for data protection and freedom of information law
- **The Privacy and Electronic Communications Regulations (PECR)** - These regulations provide a range of rules around electronic communications. AmplifyChange will most commonly follow these for direct marketing by email, campaigns and the use of cookies on our websites and emails

AmplifyChange is registered with the Information Commissioner's Office as a 'data controller', registration number ZB492195.

3. The Role of the Data Protection Officer

AmplifyChange will ensure it has a Data Protection Officer, who will take responsibility for all matters relating to data protection.

The Data Protection Officer shall:

- Inform and advise the organisation about obligations to comply with data protection laws
- Monitor compliance with the Data Protection Act 2018 and GDPR
- Have appropriate expertise or experience
- Be the primary Data Protection contact point in the organisation
- Keep the Privacy Statement current
- Advise on and monitors Data Protection Impact Assessments
- Cooperate with the Information Commissioner’s office (ICO) and is the first point of contact
- Carry out other tasks and duties, provided there is no conflict of interest, so the DPO may hold the asset register and records of the organisation as the central point for ensuring that the organisation is compliant
- Understand and advise on a risk-based approach to data processing in their organisation

AmplifyChange has engaged an external Data Protection Officer who can be reached at dpo@amplifychange.org

4. Responsibilities

AmplifyChange is the Data Controller and takes overall responsibility for compliance with the Act.

The technical security of personal data is the responsibility of AmplifyChange who may, with the agreement of the Data Protection Officer, introduce technical security requirements additional to those outlined in this policy as and when necessary.

Members of the Senior Management Team are responsible for the quality, security and management of Personal Data and Special Category Data held by their particular areas. They are responsible for ensuring that this policy is communicated and implemented within their area of responsibility.

Maintaining a central register of information assets is a key component of achieving data protection compliance. Senior Management should play a proactive role in supporting the DPO to make sure that Records of Processing Activities are accurate and up to date.

5. Processing personal data

The collection of new categories of Personal Data and/or Special Category must be approved by the Head of Operations and the Data Protection Officer and only as much should be collected as required.

When personal information is collected about data subjects, a clear explanation must be provided about how the data will be used. This may be verbally, via a sign (usually in the case of CCTV) or via a statement on a form. All forms requesting personal data, whether electronic or in paper format, will contain a Data Protection Statement, outlining who will use the data and what it will be used for, unless this is already perfectly clear elsewhere on the form. Forms must be approved by the Data Protection Officer before being printed or published on AmplifyChange's website.

All Personal Data and Special Category Data collected by AmplifyChange, or by other organisations on AmplifyChange's behalf, must be collected in accordance with AmplifyChange's Privacy Notice. A link to the Privacy Notice must be available on all webpages where personal data is collected. For personal data collected in other formats the Privacy Notice must be supplied in the most appropriate way

AmplifyChange will provide new members of staff with details of how their Personal Data and Special Category Data will be obtained, processed, disclosed and retained.

Personal Data and Special Category Data must always be collected securely. Web pages collecting personal data will always be encrypted.

6. Data subject rights

Data subjects have the following rights:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights related to automated decision making

AmplifyChange will make available the following information when requested, subject to verification of the enquirer's identity:

- Whether AmplifyChange holds any personal data relating to the enquirer and what it is
- Why it is held and for what purpose
- How long it will be held for
- Who it may be disclosed to
- The logic involved in any automated personal data processing

- Their rights concerning that data

All requests must be handled in line with the Data Rights Request Procedure and passed to the Data Protection Officer immediately. AmplifyChange will comply with written requests within one calendar month of receipt.

7. Using data

Any access to Personal Data and Special Category Data including personnel files, marketing databases, CCTV will be limited to authorised personnel only.

Personal Data and Special Category Data will be kept accurate, up to date and not be held for longer than is necessary, unless it is required for archiving purposes. Personal Data and Special Category Data will have a clear retention period. AmplifyChange's retention schedule provides further details of how long certain categories of record should be kept.

AmplifyChange will only use Personal Data and Special Category Data or the purpose for which it was collected. It will not reuse the data for any other purpose unless the consent is obtained, or if the reuse is allowed by the data protection legislation and approved by the Data Protection Officer.

8. Marketing and sharing data with third parties

Data subjects will be removed immediately from mailing lists on receipt of a written request.

Personal Data and Special Category Data Personal data will not be shared and/or sold to any outside organisation for use in direct marketing campaigns. Data may be exchanged with similar organisations for use in direct marketing only where the positive consent of the data subject and the permission of the Data Protection Officer have been obtained first.

Personal data can only be released to external enquirers or shared with other organisations with the prior approval of the Data Protection Officer and in compliance with the Act. Occasionally, there will be a legal requirement for AmplifyChange to release information to external organisations; where this is the case, applications should normally be in writing (unless the need is urgent) and be submitted to the Data Protection Officer.

All requests from third parties to view personal data held by AmplifyChange must be in writing and submitted to the Data Protection Officer.

From time to time, AmplifyChange may act as a joint data controller for personal data collected in partnership with allied organisations for a common purpose. In these cases, the collection, use and management of the data will be subject to a data sharing agreement, signed by a senior manager and approved by the Data Protection Officer.

9. Data breaches

Personal Data and Special Category Data will be stored securely and in accordance with AmplifyChange's Information Security Policy and relevant procedures.

Staff are responsible for ensuring that Personal Data and Special Category Data is kept securely and is not disclosed, either orally or in writing, to any third party without the permission of the Data Protection Officer.

All data breaches must be reported immediately to the Data Protection Officer. Breaches must be managed in accordance with AmplifyChange's Data Breach Procedure. Serious data breaches will be reported to the Information Commissioner within 72 hours.

Personal Data and Special Category Data must be disposed of confidentially and securely including both digital and print, regardless of format or media.

Breaching the UK's privacy laws can result in enforcement action by the ICO, including monetary penalties.

10. Procurement

The Data Protection Officer must approve any procurement plans for the management of personal data. This includes the purchase of new IT systems or the outsourcing of AmplifyChange functions where personal data is involved.

Business cases for new systems or outsourcing the management of personal data must include a Privacy Impact Assessment and specify the requirements for security controls. They must comply with AmplifyChange's Information Security and Management policies.

Any third-party processing personal data on behalf of AmplifyChange will be required to comply with the law and this policy. All outsourcing arrangements must be governed by a contract, which must include commitments to process personal data in line with the responsibilities of processors out in GDPR Article 28. The Data Protection Officer must approve the final contract.

If personal data is being transferred outside the UK or EEA to a country that does not have an adequacy decision, by AmplifyChange or one of its processors then a transfer risk assessment must be completed and an appropriate safeguard such as the International Data Transfer Agreement (IDTA) must be in place.

11. Staff training and Awareness

General procedures for the collection, management and disposal of personal data are available to all staff from the Data Protection Officer and via the Intranet (Box).

All staff are required to attend mandatory data protection training. Further training will be provided appropriate to the individual's role.

Staff found to be in breach of this policy will be subject to disciplinary action.

12. Monitoring and review

This policy is reviewed on an annual basis. It may be reviewed earlier to meet changes in legislation or AmplifyChange's organizational needs.

13. Revision schedule

Version	Date	Revisions
V1	June 2021 (created)	
V2	April 2024	• Revisions made in response to Data Protection Audit and in preparation for Chairty Status. • AmplifyChange is moving towards a top-level data protection policy model that uses procedures as standalone documents to allow them to be updated in a timelier fashion, as well as improving useability, when compared to a policy heavy model. Key policy documents identify areas of compliance, address the legal background and responsibilities, and provide some information before referring readers to procedures.

Definitions

Data	Any information, which is being processed automatically or recorded as part of a relevant, filing system.
Data Controller	A person or organisation who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.
Data Subject	An individual who is the subject of personal data.
Personal Data/Information	Data which relates to an identifiable living individual
Processing	Obtaining, accessing, altering, adding to, deleting, changing, disclosing or merging data and anything else, which can be done with data
Special Category Data	Information about an individual's racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health or condition, sexual life, commission or alleged commission of any offence, any proceedings for any offence committed or alleged to have been committed by him/her.

Appendix A: Associated legislation, policies and procedures

- Data Protection Act 2018
- UK General Data Protection Regulations
- Privacy and Electronic Communications Regulations

Applicable policies and procedures (available from our website or on request from the Data Protection Officer):

- Appropriate Policy Document
- Cookies Statement
- Data Protection Impact Assessment Procedure
- Data Rights Request Procedure
- Privacy Notice
- Procedure for reporting breaches
- Retention Policy & Schedule