Data Protection Policy

AMPLIFYCHANGE

Document Control	
Approved By	AmplifyChange Directors
Responsible Owner:	CEO, Operations Manager
Created:	1 June 2021
Revised:	
Approved:	
Next Review:	
Version	1

TABLE OF CONTENTS

Photo credits
Cover, right: Coalition on Violence Against Women, Kenya

1 Introduction and scope

AmplifyChange needs to keep certain information about its employees, clients, donors, and other stakeholders to enable us to deliver services. It is necessary to process information, so employees or consultants can be recruited and paid, projects delivered and legal obligations to funding bodies, government and third-party partners met. AmplifyChange recognises the importance of preserving privacy and protecting personal data and is committed to complying with the principles of the Data Protection Act 2018 (DPA18) and the EU General Data Protection Regulation (GDPR).

This policy applies to all employees, consultants, suppliers, and other representatives engaged by us in the UK or overseas. All contractors and agents acting for and on behalf of us should be made aware of this policy. This policy applies to all personal and sensitive personal data processed on computers and stored in manual (paper-based) files.

2 Policy Statement

AmplifyChange regards the lawful and correct treatment of personal information as very important to successful operations and to maintaining the confidence of all our stakeholders. We will do everything within our authority to demonstrate our commitment and endorsement of the Principles of the DPA18 and GDPR, and ensure we treat personal data and the rights of individuals with respect.

To this end, we fully endorse and adhere to the Principles of Data Protection as enumerated in the DPA18 and GDPR, and we commit to:

- Comply with both law and good practice,
- Respect individual's rights,
- Be open and honest with individuals whose data is held,
- Provide training and support for staff who handle personal data, so they can act confidently and consistently,
- Notify the Information Commissioner's Office (ICO).

To meet our responsibilities all staff and individuals who process data on behalf of AmplifyChange will:

- Ensure any personal data is collected in a fair, transparent and lawful way,
- Explain why the data is needed at the start of the point of collection,
- Ensure that only the minimum amount of information needed is collected and used,
- Ensure the information used is up to date and accurate,
- Review the length of time information is held, and
- Ensure the rights people have in relation to their personal data can be exercised.

3 General Principles of GDPR

The GDPR sets out seven key principles which AmplifyChange complies with:

- Lawful, fair and transparent processing – when the data is collected, it must be clear as to why that data is being collected and how the data will be used,
- Purpose limitation –there must be a lawful and legitimate purpose for processing the information,
- Data minimisation –data captured must be adequate, relevant and limited,
- Accurate and up-to-date processing – ensure information remains accurate, valid and fit for purpose,
- Limitation of storage in the form that permits identification – discourage unnecessary data redundancy and replication, and controls, storage and movement of data,
- Confidential and secure – protect the integrity and privacy of data by making sure it is secure (which extends to IT systems, paper records and physical security), and
- Accountability and liability – demonstrating compliance by ensuring every step within the GDPR strategy is auditable and can be compiled as evidence quickly and efficiently.

All data users must follow AmplifyChange procedures to ensure AmplifyChange complies with the fair and lawful processing of personal data.

Non-Compliance: The aim of this policy is to embed the principles of data protection throughout our operations and protect all those with whom we have a relationship with. Data privacy is relevant to and the responsibility of everyone.

The DPA is enforced in the UK by the Information Commissioner's Office (ICO). The ICO has a number of powers including the ability to fine organisations up to £17.5 million or 4% of the global annual turnover, and publicise information about data protection breaches. They can also prosecute those who commit criminal offences under the Act.

Data protection breaches may be conducted wilfully, negligently or unintentionally. Any data breach or failure to follow this policy is likely to result in disciplinary procedures being applied.

Suppliers and subsidiaries of AmplifyChange: As a matter of good practice, other agencies and individuals working with AmplifyChange, who have access to personal information, will be expected to have read and to comply with this policy. It is expected that individuals in the organisation who deal with external agencies or partners will take responsibility for ensuring an appropriate contract is in place to ensure compliance with this policy and related requirements under the GDPR.

4 Data Protection Roles and Responsibilities

For the purposes of the GDPR, AmplifyChange is the "data controller". We are wholly committed to ensuring we adhere to our responsibilities and have identified the following roles.

Data Controller
Our Board of Directors is accountable and has the overall responsibility for our compliance with data protection and determines the purposes for which, and the way, personal data are to be processed.

Data Protection Officer
Our Board of Directors has appointed a Data Protection Officer from the management team to take responsibility for the data protection policy. The Data Protection Officer has the following responsibilities:

- Briefing the Board on Data Protection responsibilities and issues,
- Reviewing Data Protection and related policies, implementing and enforcing,
- Ensuring regular checks are undertaken by managers and supervisors,
- Identifying and addressing areas where there is a risk of a data protection breach,
- Ensuring that Data Protection induction and refresher training takes place,
- Registering and corresponding with the ICO; maintaining the accuracy and currency of the organisation's notification,
- Handling data breach process and Subject Access Requests,
- Approving contracts with Data Processors,
- Approving unusual or controversial disclosures of personal data,
- Undertaking internal audits and ensuring appropriate records are maintained to demonstrate compliance and reporting to Board,
- Ensuring staff are aware of and abide by this policy, associated guidance and identifying needs for additional training, and
- Ensuring all staff are responsible for the security of information within their area and applying good information handling practice within the organisation.

All Employees/Staff
All staff who collect, process or manage information about other staff or third parties must comply with this policy and related guidance. Staff must ensure personal data is kept securely and is not disclosed to any unauthorised third party. Diligence should be applied to confidentiality requirements, particularly when determining whether the information is appropriate to disclose, and extreme care should be taken to ensure the safety of personal data.

All staff are responsible for checking any information provided to AmplifyChange about their employment is accurate and up to date. They should inform their manager of any changes to personal information provided, such as a change of address, or whether the information we hold has errors or is inaccurate. All employees who hold or process personal data are considered to be "Data Users".

Consultants, Suppliers and Others
AmplifyChange engages suppliers who may be contractors, independent consultants, temporary workers, associates and interns. All those who undertake work on behalf of us are considered to be "Data Users", and must

comply with this policy and understand their obligations and responsibilities to ensure compliance with Data Protection.

Provision will be made in contracts with external providers and consultants to ensure compliance with this Data Protection Policy and the GDPR. Where third parties undertake work on behalf of us, we remain the data controller and must take appropriate measures to ensure the contract is explicit on third party obligations.

5 Data Protection additional definitions

To help understand data protection and to adhere to the rules, the following section provides definitions of the key terms used throughout the in the policy.

Information Commissioner's Office: The ICO is the regulatory body which oversees compliance with the Act. It:

- Sets guidance for organisations to help them and their staff comply with the Act,
- Provides advice to organisations on how to comply with the Act,
- Investigates complaints made by individuals who believe there has been a breach, and
- Has power to take action against organisations who do not comply, or where there has been a breach, including enforcement notices, monetary fines and criminal sanctions.

Data Subject: A person or individual who is the subject of personal data. Within the workplace, they may be current employees, people applying for jobs or former employees. Data subjects might also be customers, suppliers, clients or other people about whom information is held. The Act does not count as a data subject an individual who has died or who cannot be identified or distinguished from others.

Data Processor: Means any person (other than an employee), who processes data on our behalf. Data Processors must also ensure they follow the principles of the act and make sure information is handled correctly; data processors will include organisations processing payroll, IT providers or other services outsourced by the organisation.

Data Processing: The term processing refers to a wide range of actions relating to personal data which includes obtaining, holding, recording, consultation or retrieving the data, or doing work on the data such as organising, adapting, changing, disclosing, erasing or destroying it. Any activity or operation carried out in relation to data is likely to fall within the definition of processing. AmplifyChange also uses external organisations to process data on our behalf (IT, payroll etc.) and these organisations are classed as Data Processors. AmplifyChange maintains responsibility for any breaches made by data processors.

Data User: All staff and other individuals who process date on behalf of AmplifyChange are a data user. Where your role requires you to process personal data, you are a data user and must comply with all the data protection principles.

Data Recipient: Any person to whom the data is disclosed including any employee or agent of the data processor. The data controller' notification to ICO must include any description of any "recipient or recipients to whom the data controller intends or may wish to disclose the data".

Personal Data Third party: In relation to personal data, means any other person other than:

- the data subject,
- the data controller, or
- any data processor, or
- other person authorised to process data for the data controller or processor.

6 Type of Information Processed

Data is collected and used for many purposes, of which these are the main categories:

- Obligations under the employment contract, (recruitment, training, appraisal, remuneration, welfare etc.),
- Legitimate business purposes, (due diligence, performance monitoring, financial monitoring and decision-making, administration and security arrangements etc.),
- Legal and regulatory requirements, and
- Provision of services to our donor and clients though grant agreements and service contracts with third parties.

AmplifyChange collects personal data in many ways including but not limited to application forms, CVs, letters, emails, appraisals, due diligence, payment information etc. This data is processed as part of our everyday operations. In all cases, there should be valid and explicit reasons for collecting personal data, for holding and processing and for how long it is held.

Whilst personal data can take many forms, the typical types of personal data processed for normal business operations includes the following:

- Personal details of staff and consultants,
- Personal banking information and salary or fee-earning history,
- Organisational financial information including salaries,
- Previous and current employment related information and disclosures, and
- Sensitive medical information as required for employment purposes or related to travel precautions such as disclosure of any relevant medical conditions that should be known by the employers or contracting authority.

If an individual does not consent to certain types of processing (i.e. database checks as part of integrity due diligence), appropriate action must be taken to ensure that the processing does not take place.

Personal data register and personal data flows
As per the GDPR guidelines, AmplifyChange will maintain a personal data register, which includes the following information**:**

- Types of personal data collected,
- The retention periods for each type of collected personal data,
- The purposes for collection of each type of personal data,
- The systems used for processing and storage of personal data including their security measures, and
- The information asset owner responsible for the data.

Exemptions
AmplifyChange's approach is to assume that all personal information collected and processed is subject to the Data Protection Act. However, in certain circumstances, particularly where this involves some public interest, data may be disclosed to third parties. The majority of these exemptions only allow disclosure and processing of personal and sensitive personal data where specific conditions are met. Please refer to the Data Protection Officer if in doubt.

7 Data Collection and Rights of Access

Where AmplifyChange collects personal data, the AmplifyChange Privacy Notice will be available to the data subject at the time of collection, or as soon as practicable after. This will be a link to the web page or in hard copy.

Where AmplifyChange engages third party organisations to process data on our behalf, we will ensure all contracts with data processors contain model contracts to ensure data processors comply with our instructions and obligations under the GDPR. We will ensure we choose data processors who provide sufficient guarantees in respect of security measures, and they comply with obligations equivalent to those imposed on AmplifyChange as the Data Controller.

Transferring Data: Information that we collect may be stored, processed and transferred between any of the countries in which we operate. AmplifyChange, in our normal course of operations, will undertake transfer of data to countries outside of the European Economic Area (EEA). This is necessary in the work we do, and in our organisational structure. Our clients, partners and other stakeholders are often located in countries outside of the EEA. As such, AmplifyChange takes steps to ensure that we comply with all the principles of the DPA and GDPR when transferring data.

Sharing Data: AmplifyChange shares personal data within the organisation and with external organisations to achieve our obligations under our employment and other contracts. When sharing information internally and externally, it is the responsibility of the requesting and receiving members of staff to consider whether they have the authority to access/disclose the information. Advice should be sought from relevant information asset owner or the Data Protection Officer. When sharing personal data externally, we must comply with the GDPR and ensure we treat individuals fairly. Before sharing personal data, all staff must check with the information asset owner or Data Protection Officer. When in doubt, advice should be sought from the ICO. The personal data should not be shared unless there is the highest level of certainty that the sharing is compliant with GDPR, which means there is a clear legitimate reason why the information should be shared, and all eight data protection principles are adhered to.

Data Subject Access Request (SAR)
The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data as well as other supplementary information. It helps individuals to understand how and why you are using their data, and check you are doing it lawfully.

The Data Protection Officer is responsible for preparing and complying with SARs. Any requests should be sent immediately to the Data Protection Officer who will log the request and follow the process to clarify the request and respond with the timeframe specified by the ICO.

Exemptions: The Freedom of Information Act (FoIA) does not currently apply specifically to private organisations. However, as AmplifyChange provides contractual services to Government Bodies, it may be deemed that we are holding information on behalf of a public body. Where such public body receive a FoIA request this may result in AmplifyChange being required to disclose confidential information and intellectual property. Any requests received should immediately be directed to the Data Protection Officer or the CEO.

8 Data Management

AmplifyChange aims to ensure that data is accurate, reliable, ordered, complete, useful, up-to-date and accessible. As soon as a data is created or received, an appropriate record keeping system should be implemented. All data records should be available and accessible with the appropriate access levels assigned for the requirements of operations respecting the principles of confidentiality and limiting duplication. The record keeping system should be designed to meet the following standards.

Storage and handling data records: All data should be stored on media that ensures their security, integrity, reliability, usability, and authenticity and in a way that takes account of the records' specific physical properties. Storage conditions and handling processes should ensure the records are protected from unauthorised access, loss, or destruction and from theft.

Data access: Access to records should be governed in a way that reflects needs and requirements and ensure there is no opportunity for the records to be disclosed, deleted, altered or destroyed, either accidentally or intentionally.

Tracking data records: The record keeping system must allow retrieval, monitoring and disposal of data when records are no longer needed. Any modifications or alterations to data records should be monitored with accurate version control system to track changes.

Data Suspension: The data should be immediately suspended in the event of litigation, claim or dispute where AmplifyChange is involved. The suspension of data means preserving information potentially relevant to litigation, investigations or other disputes, as well as any steps AmplifyChange must take to ensure that data maintains its evidentiary integrity.

Data Retention and disposal: An approach to data retention and disposal is required to ensure that data is managed through its life cycle from creation or receipt, through to disposal. Good data management relies on the following:

- Understanding what data needs to be captured and stored,
- Understand how long we need to retain data, and
- Put in place data tracking mechanisms with and data disposal carried out at the right time.

Each staff member should seek to understand the data retention requirements for their data based on statutory requirements or client contract requirements. All data retention periods will be recorded in the personal data register.

Data disposal methods: Once records have been retained for the applicable period, they should be prepared for disposal:

- Paper records should be shredded.
- Electronic data should be deleted permanently (including the bins) and not available for retrieval.
- Electronic data contained on servers and hard drives should be deleted and overwritten.
- Electronic data contained on all other media should be destroyed by the physical destruction of that media.

Staff should take into account the following considerations when selecting any method of disposal:

- Under no circumstances should paper documents or removable media (CDs, DVDs, discs, etc.) containing personal data or confidential information be binned or deposited in refuse tips. To do so could result in the unauthorised disclosure of such information to third parties and render AmplifyChange liable to action under the Data

Protection Act. Such documents should be destroyed on site (e.g. by shredding) or placed in "Confidential Waste" refuse bins.
- Deletion -the ICO has advised that if steps are taken to make data virtually impossible to retrieve, then this will be regarded as equivalent to deletion.
- Recycling -wherever practicable disposal should further recycling, in-line with AmplifyChange's commitment to the environment.

Training: Training on Data Protection is mandatory for all employees. All new employees will receive training on this policy and the related policies and procedures referred to above.

Refresher training will be conducted on a regular basis for existing employees. Managers should include data protection on their agendas for team meetings to ensure we are reinforcing our desire to respect the information of data subjects and promote best practice and consistent standards.

Complaints: If anyone is dissatisfied with the way in which we have handled personal data, please contact the Data Protection Officer. If, after this, you are still dissatisfied with how AmplifyChange has managed your data, you also have the right to lodge a complaint with the ICO. You can find details about how to do this at https://ico.org.uk/concerns/ or by calling ICO' helpline on 0303 123 1113.

9 Data Protection Breaches

AmplifyChange is committed to preventing data breaches and for managing them efficiently if they do occur. The following section on managing a data breach is intended to mitigate the impact of any data breaches and to ensure that they are handled correctly.

Data breach identification and containment: Reporting incidents fully and with immediate effect is essential for the protection of AmplifyChange, our staff, customers, clients and third parties and is of the utmost importance for legal regulatory compliance.

If a breach is identified or just suspected, it should be immediately reported to the Data Protection Officer, who will immediately review the situation to ascertain the cause, scale and severity of the breach and decide upon an immediate containment action. Where there has been a loss of personal data, the Data Protection Officer will notify the data subject and the ICO in line with the reporting requirements.

Data breach response: Once the breach has been contained and if necessary, reported to the data subject and ICO, the Data Protection Officer will review the circumstances that led to the data breach and identify any further mitigations or response plans to prevent any further incidents.

Breach Recording: All suspected data breaches should be logged and recorded on a data breach register. An incident form should be used for any incidents to capture the details, the containment measures and the response.

Breach Notification: AmplifyChange understands its obligations to report data breaches. The Data Protection Officer is responsible for ensuring that data breaches falling within the notification criteria are identified and reported without undue delay. When a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, we will always communicate the personal data breach to the data subject without undue delay, in a written format and in a clear and legible format. The notification shall include:

- The nature of the personal data breach,
- The name and contact details of our Data Protection Officer and/or any other relevant point of contact (for obtaining further information),
- A description of the likely consequences of the personal data breach, and
- A description of the measures taken or proposed to be taken to address the personal data breach (including measures to mitigate its possible adverse effects).

We reserve the right not to inform the data subject of any personal data breach where we have implemented the appropriate technical and organisational protection measures, which render the data unintelligible to any person who is not authorised to access it (i.e. encryption, data masking etc.); or where we have taken subsequent measures, which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise. If informing the data subject of the breach involves disproportionate effort, we reserve the right to instead make a public communication whereby the data subject(s) are informed in an equally effective manner.