Data Breach Policy

Document Ref:	Data Breach Policy
Version:	2.0
Date of Version:	**17 April 2020**
Author:	**Lucian-Gabriel Burcea**
Approved by:	Lucian-Gabriel Burcea (DPO)
Confidentiality Level:	Internal: **Uncontrolled if printed**

Document Overview

This Subject Access Request Form is a controlled document and is maintained on the server as read-only. The Data Protection representative must ensure that all amendments are circulated, and obsolete copies removed and filed. Hard copies used for training and internal auditing are controlled and distributed as follows.

Circulation List

Date	Distribution List
	All Staff

Amendment History

This document is reviewed periodically, at least annually, and is retained for a period of 5 Years. Amendments and revisions are distributed to the named holders. The history of amendments and the issue of revisions are recorded below.

Date	Amend. No.	Page No.	New Issue No.	Reason for Change	Authorised by

Copies of this document other than those listed above will not be revised; such copies will be marked as **UNCONTROLLED**.

Key Roles and Responsibilities

All users, including all A New Direction employees, temporary employees, and third parties working with us or on our behalf, must be aware of this policy and the procedure outlined.

If you become aware of a security incident (e.g. you lose a hardcopy of a document that contains personal data or send an email with personal data by mistake) you must inform the following immediately:

Role	Name	Email address
Internal Data Protection Lead	Hasina Allen	dataprotection@anewdirection.org.uk
Data Protection Officer	Lucian-Gabriel Burcea	lgburcea@clearcomm.org

If you are ever in any doubt about whether something is a data security incidence always inform the Internal Data Protection Lead and Data Protection Officer immediately.

1. Scope of policy

This procedure applies in the following events:

1. A personal data breach as defined by Article 33 'Notification of a personal data breach to the supervisory authority', of the GDPR and

2. A personal data breach pursuant to Article 34 ‘Communication of a personal data breach to the data subject’ of the GDPR.

2. Responsibility

All A New Direction employees, temporary employees/freelancers, and third parties working with us or on our behalf, must be aware of this policy and the procedure outlined and are required to follow the procedure should a personal data breach incident occur.

The Data Protection Officer and Internal Data Protection Lead are responsible for ensuring the Data Breach Procedure outlined in this policy is followed in the event of a data breach.

3. Definition

What is a personal data breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

4. Understanding data controller vs. data processor

There is a distinction under the GDPR between a ‘data controller’ and a ‘data processor’. This is because different organisations involved in processing personal data have varying degrees of responsibility. An organisation must choose whether it is a data controller or a data processor.

Most of the time A New Direction will be the data controller, where we are collecting personal data directly from our stakeholders/participants.

Occasionally A New Direction will be the data processor, for example where we are a delivery partner on a project and have personal data collected by another organisation has been shared with us.

5. Data Breach Notification Procedure

1. Data processor to data controller

All personal data breaches by A New Direction must be notified to the appropriate data controller immediately.

Where A New Direction is the data controller (which is the majority of the time), any member of staff or individual processing data on AND's behalf (including freelancers) must inform DPO and IDPL as soon as they are made aware of a personal data breach. If you are ever unsure, please still inform the IDPL as soon as possible.

The Data Protection Officer ('DPO') must record the communication of the breach in the Data Breach Register, stating how the notification was made (whether by email, telephone call etc.), to whom and how the confirmation of receipt was provided.

2. Data controller to supervisory authority

If the DPO decides that a risk is considered likely, A New Direction is required to report the personal data breach to the supervisory authority immediately and in any event, no later than 72 hours after they have been aware about the breach. If the notification is made outside of the 72 hour window, A New Direction is required to provide reasons for the delay.

A New Direction is required to provide the following to the supervisory authority:

- A description of the nature of the personal data breach;
- The categories of personal data that have been affected by the breach;
- The number, which may be approximated if necessary, of data subjects affected by the breach;
- The number, which may be approximated if necessary, of personal data records affected by the breach;
- The name and contact details of the DPO;
- The likely outcomes of the personal data breach;
- Any measures taken by A New Direction to address and/or mitigate the breach; and
- All other information regarding the data breach.

The DPO must record the communication of the breach in the Data Breach Register, stating how the notification was made (whether by email, telephone call etc.), to whom and how the confirmation of receipt was provided.

3. Data controller to data subject

If it is likely that there will be a high risk to the affected data subject's rights and freedoms under the GDPR, A New Direction is required to provide immediate notification to the relevant data subjects.

The notification to the data subject must be made in clear and plain language and must include the following:

- A description of the nature of the personal data breach;
- The categories of personal data that have been affected by the breach;
- The number, which may be approximated if necessary, of data subjects affected by the breach;
- The number, which may be approximated if necessary, of personal data records affected by the breach;
- The name and contact details of the DPO;
- The likely outcomes of the personal data breach;
- Any measures taken by A New Direction to address and/or mitigate the breach; and
- All other information regarding the data breach.

If notification would require A New Direction to implement a disproportionate amount of effort, a public communication or other similar measure may suffice, so long as all data subjects are effectively informed.

It is possible that the supervisory authority may require A New Direction to communicate the personal data breach to the data subject, should there be an element of high risk involved.

A New Direction must use appropriate measures, such as encryption, to ensure that all personal data is secure and cannot be accessed by those without the requisite authority.

A New Direction must also take subsequent measures to ensure that the risk to the rights and freedoms of the data subject are no longer an issue.

6. Document Management

A New Direction is the owner of this policy document and must ensure that it is periodically reviewed according to the review requirements contained herein.

The latest version of this policy document dated 17 April 2020 is available to all employees of A New Direction on the corporate intranet.

Name of Data Protection Officer:	Lucian-Gabriel Burcea
Date:	28 May 2020