31. Data Protection Policy

Table of Contents

1. Overview

This policy outlines A New Direction's commitment to the accurate, secure and lawful processing of personal data; the processes and procedures we have in place to ensure this; and our expectations around data protection for anyone who works for or on behalf of A New Direction.

In order to operate efficiently and measure our impact, we collect information about the people we work with. This includes current, past and prospective employees; freelancers; suppliers and contractors; and members of the public.

We regard the lawful and correct treatment of personal data as very important to successful operations, and to maintaining confidence and trust with the people we work with. We ensure that A New Direction treats personal information lawfully and correctly.

Data protection is everyone's responsibility. Everyone who works for or on behalf of A New Direction is expected to read and adhere to this policy.

Purpose

This policy outlines our data protection processes and procedures, and how we will ensure that:

- everyone managing and handling personal information understands that they are responsible for adhering to good data protection practice
- procedures for collecting, processing and storing personal data are secure, clear and in compliance with legislation and approved procedures
- staff who collect or process personal data are appropriately trained

This policy helps to **protect A New Direction from some very real data security risks** including:

- **Breaches of confidentiality**, such as information being given out inappropriately;
- **Failing to offer choice**, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage**, for example if hackers successfully gained access to sensitive data due to access caused by a member of staff accessing a phishing link.

Policy Scope

This policy applies to **anyone working for or on behalf of A New Direction**, including all employees, freelancers, contractors, volunteers and suppliers.

What data does this policy apply to?

This policy applies to all data A New Direction holds relating to identifiable individuals, even if that information technically falls outside of the General Data Protection Regulations. This can include:

- names of individuals;
- contact details, including addresses, telephone numbers and email addresses;
- health information;
- employment data; and
- any other information relating to individuals.

Roles and Responsibilities

Key Roles:

Everyone who works for or with A New Direction has the responsibility for ensuring data is collected, stored and handled appropriately, however there are some key roles that have a particular responsibility for data protection.

Internal Data Protection Lead (IDPL):
The Planning and Operations Manager is A New Direction's Internal Data Protection Lead (IDPL).

The IDPL has overall responsibility for the administration and implementation of the Data Protection Policy.

Data Protection Officer (DPO):
A Data Protection Officer (DPO) is an independent expert in data protection who reports to the highest management level.

A DPO:

- assists an organisation to monitor internal compliance and informs and advises on your data protection obligations,
- provides advice regarding Data Protection Impact Assessments (DPIAs),
- acts as a contact point for data subjects and the supervisory authority, and
- can help demonstrate that compliance and security are part of the enhanced focus on accountability.

A DPO can be an existing employee or externally appointed.

A New Direction has appointed a certified and experienced DPO through ClearComm, a data protection solutions specialist (March 2020).

DPO Details: Lucian-Gabriel Burcea , lgburcea@clearcomm.org

Any breach of the GDPR or this policy, will be considered as a breach of the disciplinary policy and could also be considered a criminal offence, potentially resulting in prosecution.

Directors are responsible for:

- Assuming authority for the compliance of the employees within their team

Senior Management are responsible for:

- Supporting Directors with ensuring compliance of employees within their team
- Developing and encouraging good information handling practices within A New Direction.
- Specific responsibilities are set out in individual job descriptions.

Each individual who works for or on behalf of A New Direction is responsible for:

- Ensuring data is collected, stored and handled appropriately.
- Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.
- All third parties who require access to personal data will be required to sign a confidentiality agreement before access is permitted. This agreement will ensure that the third party has the same legal obligations as A New Direction. This will also include an agreement that A New Direction can audit compliance with the agreement.

The Internal Data Protection Lead is responsible for:

- Day to day compliance with this policy.
- Supporting Senior Management to develop and encourage good information handling practices across A New Direction.
- Oversight of organisational-wide GDPR and Data Protection Training.

The Data Protection Officer is responsible for:

- Ensuring that A New Direction complies with the GDPR in relation to all aspects of data processing.
- Direct responsibility for data protection policies and procedures, including Subject Access Requests.
- Supporting the team to comply by acting as a point of contact for enquiries about GDPR compliance and providing guidance and advice.
- Ensuring that all necessary actions are taken to ensure personal information is accurate and up to date. This should also consider the volume of data collected, the speed with which it might change and any other relevant factors.
- Reviewing, at least once a year, all the personal data processed by A New Direction, held in the Data Register. The DPO will note any data that is no longer required in the context of the registered purpose and will ensure that it is appropriately removed and securely disposed of.

Key considerations

Data access and sharing:

- The only people able to access data covered by this policy should be those who need it for their work.

- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should not be shared informally. When access to confidential information is required, employees should request it from their line managers.

Data security:

- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used, and they should never be shared.

Data accuracy:

- Personal data must be accurate and kept up to date.
- Data should be regularly reviewed and updated as necessary. Any data that is inaccurate or likely to be inaccurate must be removed.

Data protection training and compliance:

- Everyone working for or on behalf of A New Direction is expected to read and adhere to the processes and procedures outlined in this policy. Everyone is expected to confirm they have read this policy as part of their induction and review the policy annually.
- A New Direction will provide training to all employees to help them understand their responsibilities when handling data and relevant data protection regulations.
- Senior management are responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

2. Data protection and the law

Data protection legislation regulates the way that we handle the personal data that we collect, hold and process and gives certain rights to people whose personal data we may hold.

GDPR and the Data Protection Act

It is our responsibility to ensure that information and data held on A New Direction's databases and systems complies fully with the principles of the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') and of the Data Protection Act 2018 ('the Act').

Both the GDPR and the Act requires that anyone who collects, processes, and stores personal information must ensure that the information (e.g. names, addresses, other information kept on individuals) is:

- secure
- accurate and up to date
- only kept for legitimate reasons
- only kept for as long as is necessary
- used for legitimate purposes, and
- not passed on to third parties without the consent of the individual.

In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities, government agencies and other bodies.

This personal information must be dealt with properly however it is collected, recorded and used – whether on paper, electronically or recorded on other material - and there are safeguards to ensure this within the GDPR and the Act.

The data controller
A data controller is the individual or legal person who controls and is responsible to keep and use personal data in paper or electronic files.

A New Direction is the data controller as defined by relevant data protection laws and regulation.

What is personal data and special category data?

Personal data is information that relates to an identified or identifiable individual.

What identifies an individual could be as simple as a name or a number or could include other identifiers such as an IP address or a cookie identifier, or other factors. If it is possible to identify an individual directly from the information you are processing, then that information may be personal data.

Special category data is personal data that needs more protection because it is sensitive.

The GDPR Defines special category data as:

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- personal data revealing trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- data concerning health;
- data concerning a person's sex life; and
- data concerning a person's sexual orientation.

More information can be found on the Information Commissioner's Office Website here: ICO guide to data protection – what is personal data?

Privacy Electronic Communication Regulations 2003

The Privacy and Electronic Communications (EC Directive) Regulations 2003 ('PECR') are derived from European law. They implement European Directive 2002/58/EC, also known as 'the e-privacy Directive'.

The e-privacy Directive complements the general data protection regime and sets out more-specific privacy rights on electronic communications. It recognises that

widespread public access to digital mobile networks and the internet opens up new possibilities for businesses and users, but also new risks to their privacy.

PECR have been amended seven times. This policy covers the latest version of PECR, which came into effect on 9 January 2019, with some updates to cover changes made by the GDPR from 25 May 2018.

The EU is in the process of replacing the e-privacy Directive with a new e-privacy Regulation to sit alongside the GDPR. However, the new Regulation is not yet agreed. For now, PECR continues to apply alongside the GDPR. Post Brexit the UK is unlikely to deviate from this and it remains in effect until further notice.

Other relevant regulations

Most businesses hold personal data on their customers, employees and partners. The explosion in the use of the Internet, electronic communication and computerisation of business data has led to an increase in the importance of privacy. Breaches of computerised data security have prompted the introduction of legislation on a national and European level.

These include:

- Human Rights Act 1998
- Freedom of Information Act 2000
- Privacy and Electronic Communications Regulations 2003
- Regulation of Investigatory Powers Act 2000
- Telecommunications (Lawful Business Practice) Interception of Communications Regulations 2000
- The Act.
- Computer Misuse Act 1990.
- GDPR.

The GDPR replaces the Data Protection Directive (Directive 95/46/EC) ('the Directive') and supersedes the laws of individual Member States that were developed in compliance with the Directive. Its purpose is to protect the 'rights and freedoms' of living individuals, and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

3. Lawful Processing of Personal Data:

A New Direction collects, holds and processes all personal data in accordance with the lawful processes under GDPR.

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever personal data is to be processed:

a) **Consent:** free, specific and informed or unambiguous consent for personal data to be processed for a specific purpose;
b) **Contract performance:** the processing is necessary for the performance of a contract an individual has with A New Direction, which had asked them to take specific steps before entering into a contract;

c) **Compliance with legal obligation:** the processing is necessary for A New Direction to comply with tax or social security obligations, and employment law (not including contractual obligations);
d) **Protection of vital interests:** the processing is vital to an individual's survival;
e) **Public interest:** the processing is necessary for A New Direction to perform a task that is in the public interest or for its official functions, and the task or function has a clear basis in law; and
f) **Legitimate interests:** the processing is necessary for A New Direction's legitimate interests, or the legitimate interests of a third-party, unless there is a good reason to protect the individual's personal data that overrides those legitimate interests.

Consent

Consent is one lawful basis for processing, and explicit consent can also legitimise use of special category data.

Genuine consent should put individuals in control, build trust and engagement, and enhance your reputation.

A New Direction understands valid consent to be:

- freely given; this means giving people genuine ongoing choice and control over how you use their data.
- obvious and require a positive action to opt in.
- prominent and clear, distinct from other terms and conditions,
- concise and easy to understand, and user-friendly.

In addition, A New Direction understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them.

Consent is not valid when:

- obtained under duress or based on misleading information
- inferred from non-response to a communication.
- explicit written consent has not been obtained (for special category data). unless an alternative legitimate basis for processing exists.

The consent of the data subject can be withdrawn at any time.

Obtaining consent

Consent to process personal and sensitive data is obtained routinely by A New Direction using standard consent documents. For employees, this may be through a contract of employment or during induction. Where special category data is concerned, explicit written consent is required.

Where A New Direction provides online services to children, consent must be obtained from their legal parent or guardian authorisation must be obtained. This requirement applies to children under the age of 16.

Collecting of consent must also be considered when A New Direction's website places cookies on the users' device. The collection of data is done automatically via cookies when users visit A New Direction' website, in line with cookie settings in the users' browser and their customised cookie settings.

4. Data use and access

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended;
- Personal data should not be shared informally. It should never be sent by email, as this form of communication is not secure – if data must be shared it should be via SharePoint in an encrypted (password protected) document.
- Data must be encrypted before being transferred electronically;
- Personal data should never be transferred outside of the European Economic Area; and
- Employees should not save copies of personal data to their own computers or external hard drives. Always access and update the central copy of any data, accessed via SharePoint or Salesforce.

5. Security and storage

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. These controls have been selected based on identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed. Security controls will be subject to audit and review.

All A New Direction staff that are responsible for any personal data which A New Direction holds must keep it secure to ensure that it is not disclosed under any conditions to any third party unless that third party has been specifically authorised by A New Direction to receive that information and has entered into a Confidentially or Information Sharing Agreement.

Personal data must be processed in a manner that ensures its security

Everyone is expected to follow these guidelines to ensure that data is processed in a manner which ensures its security:

- When accessing personal data, care must be taken to ensure that PC screens and terminals are not visible except to authorised staff of A New Direction.
- A New Direction held personal data must not be processed on any devices except those provided by A New Direction, without explicit authorisation from the Senior Management Team.
- Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit written authorisation. As soon as manual records are no longer required for day-to-day work, they must be moved to secure archiving.

- Personal data may only be deleted or disposed of in line with the Data Retention Procedure.

Passwords: A New Direction staff must change their password every three months and must not share their login information with anyone in or outside the organisation.

- All passwords used to protect personal data should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols.
- Under no circumstances should any passwords be written down or shared between A New Direction, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords.

Key security risk – phishing: One of the biggest email-based threats is phishing, which can be mitigated with the help of all staff. Phishing emails often look legitimate enough to bypass spam filters, meaning the only thing standing between A New Direction and a data breach, is a member of staff who is able to recognise the threat

Both the GDPR and the Act require that personal data is securely handled, therefore, **it is considered a disciplinary offence to save personal data on local drives or laptop desktops without authorisation. If there is a truly exceptional circumstance, staff should consult their line manager.**

A New Direction shall ensure that the following measures are taken with respect to IT and information security:

- All software (including, but not limited to, applications and operating systems) shall be kept up to date. A New Direction IT support shall be responsible for installing any and all security-related updates as soon as reasonably and practically possible.
- No software may be installed on any A New Direction owned computer or device without the prior approval of a Manager or the DPO.
- Personal data shall not be transferred to a country or territory outside the European Union Member States unless that country or territory ensures an adequate level of protection for the 'rights and freedoms' of data subjects in relation to the processing of personal data.

Personal data must be stored safely and securely

All personal data should be accessible only to those who need to use it and should be stored in line with the principles outlined below. Questions about storing data safely can be directed to the DPO or IT Support.

Digital Copies

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be stored in approved secure systems, Salesforce, PeopleHR, or in a password protected file on SharePoint.

- Data should only be stored on designated systems and should only be uploaded to an approved cloud computing service.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- Data should not be stored on removable media (like a USB, CD or DVD).
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard back up procedures.
- All servers and computers containing data should be protected by approved security software and a firewall.
- You should never access or download personal data onto an unauthorised device.

Hard Copies

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot access or read it.

These guidelines also apply to data that is usually stored electronically but have been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

Removal of confidential personal data offsite is not usually permitted. In certain exceptional circumstances, and only with Director approval, personal data may be downloaded onto local drives or computer desktops. Before doing this staff must always obtain authorisation from the Director of their team. Staff should make requests in writing stating why downloading or transportation of data is required, physical address of storage location, and identify any risks associated with transportation and offsite storage.

6. Data accuracy

The law requires A New Direction to take reasonable steps to ensure data is kept accurate and up to date.

- Staff should take every opportunity to ensure data is updated (i.e. updating an email address or contact number after being notified of a change.)
- A New Direction will make it easy for data subjects to update the information A New Direction holds about them. Data should be updated as inaccuracies are

discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

- It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.
- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- It is the Senior Communication Manager's responsibility to ensure marketing databases are checked against industry suppression files every six months.

7. Data Breaches

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.

What happens if there is a personal data breach?
All employees must report a breach, or suspected data breach to their manager and/or the Data Protection officer.

In the event of a personal data breach, A New Direction will follow the procedure outlined in the Data Breach Policy.

When a personal data breach has occurred, A New Direction will assess the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk, then the DPO must notify the ICO – this is highly likely. If it is decided that it is not necessary to report the breach, we still need to be able to justify this decision, so you should document it.

A notifiable breach must be reported to the ICO without undue delay, but not later than 72 hours after becoming aware of it

8. Risk Assessment in relation to GDPR

A New Direction needs to ensure that it is aware of any risks associated with the processing of all types of personal information.

A Risk Assessment procedure has been implemented and is used by A New Direction to assess any risk to individuals during processing of their personal information. Assessments will also be completed by A New Direction for any processing that is undertaken on their behalf by any third-party organisation.
A New Direction will also, through the application of the Risk Assessment procedure, ensure that any identified risks are managed appropriately to reduce the risk of non-compliance.

Where processing of personal information may result in a high risk to the 'rights and freedoms' of natural persons, A New Direction shall complete a data protection impact assessment (DPIA), prior to conducting the processing, to ensure the personal information is protected. This assessment may also be used to apply to several similar processing scenarios with a similar level of risk.

Where, because of a DPIA, A New Direction will process personal information in a manner that may cause damage and/or distress to the data subjects, the DPO must review the process before A New Direction proceeds to process the information. If the DPO decides that there are significant risks to the data subject he will escalate to the ICO for final guidance. The organisation shall apply selected controls for the ISO/IEC 27001 Annex A to reduce risk. This should also reference A New Direction's risk acceptance criteria and the requirements of the GDPR.

9. Disclosing data and providing information

Providing information

A New Direction aims to ensure that individuals are aware that their data is being processed, and they understand:

- How the data is being used; and
- How to exercise their rights.

To these ends, the company has a Privacy Policy, setting out how data relating to individuals is used by the company.

Subject access requests

All individuals who are the subject of personal data held by A New Direction are entitled to:

- Ask what information the company holds about them and why;
- Ask how to gain access to it;
- Be informed how to keep it up to date; and
- Be informed how the company is meeting its data protection obligations.

If an individual, contacts the company requesting this information, this is called a subject access request.

A New Direction will follow the procedure outlined in the Subject Access Request Policy.

The subject access requests are free of charge, unless there are excessive requests coming from a certain individual.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Only under the above circumstances, A New Direction will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

10. Retention and disposal of data

A New Direction has a Data Retention Policy, which includes guidelines about the disposal of data, and will ensure that the processes in this policy are adhered to in the retention and disposal of data.

Retention

A New Direction shall ensure that the following measures are taken with respect to the storage of personal data (including, but not limited to, personal data relating to employees):

- all electronic copies of personal data should be stored securely using passwords and data encryption wherever possible;
- all hard copies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;
- all personal data stored electronically should be backed up on A New Direction's internal systems, with backups stored onsite and offsite. All backups should be encrypted.
- no personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to A New Direction or is a personal device belonging to an employee without the formal written approval of the Director for your team. In the rare event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary; and
- personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of A New Direction where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the GDPR (which may include demonstrating to A New Direction that all suitable technical and organisational measures have been taken).

Disposal

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to the Data Retention Policy.

11. Complaints

A Data Subject has the right to complain at any time to A New Direction if they have concerns about how their information is used. If they wish to lodge a complaint this should be directed to the DPO following the complaints procedure using a complaint form supplied by A New Direction.

A Data subject also has the option to complain directly to the Information Commissioners Office. Details of the options for lodging a complaint is provided by A New Direction within the Privacy Policy available on our company website.

Document Management and Review

This document is valid as of 14th September 2020.

This document is reviewed periodically and at least annually to ensure compliance with the following prescribed criteria.

- General Data Protection Regulation
- Legislative requirements defined by law, where appropriate

This Policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Act and the GDPR.

The Data Protection Policy will, under normal circumstances, be managed and reviewed annually. The reviews to the Policy will be subject to scrutiny and, from time to time, updates and re-issues will be circulated.

However, the Policy will be reviewed sooner in the event of any one or more of the following:

- Weakness in the Policy is highlighted
- Weaknesses in hardware and software controls are identified
- In case of new threat(s) or changed risks
- Changes in legislative requirements
- Changes in Government, company or other directives and requirements.

Date written	July 2020
Author	Lucian-Gabriel Burcea and Hasina Allen
Version	2.0
Date approved	14/09/2020 (Finance and HR Subcommittee)

Appendix I: Safeguards for transferring data outside of the EEA

An assessment of the adequacy by the data controller considering the following factors:

- the nature of the information being transferred;
- the country or territory of the origin, and destination, of the information;
- how the information will be used and for how long;
- the laws and practices of the country of the transferee, including relevant codes of practice and international obligations; and
- the security measures that are to be taken about the data in the overseas location. (This is a UK-specific option.)

Binding corporate rules

A New Direction may adopt approved Binding Corporate Rules for the transfer of data outside the EU Member States.

Model contract clauses

A New Direction may adopt approved model contract clauses for the transfer of data outside of the EU Member States. If A New Direction adopts the model contract clauses approved the relevant Supervisory Authority, there is an automatic recognition of adequacy.

Ad Hoc contractual clauses

A New Direction may adopt ad hoc contractual clauses that will have to be approved by the ICO. They allow the A New Direction to individually tailor the transfer to its needs, however, the provisions for such clauses may differ at the member state level.

Exceptions

In the absence of an adequacy decision, including binding corporate rules, for the transfer of personal data to a third country, or an international organisation, it shall take place only on one of the following conditions:

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims;
- the transfer is necessary to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
- the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case.

A list of countries that satisfy the adequacy requirements of the Commission are published in the Official Journal of the European Union and in the GDPR.