PERSONAL DATA BREACH MANAGEMENT POLICY

STATEMENT

Your Chapter Ltd. ('we', 'us', and 'our') is committed to respecting and protecting the privacy of individuals and to fully complying with all the requirements of Data Protection Legislation.

We have appointed a Data Protection Officer (DPO) who can be contacted via dpo@yourchapter.co.uk

SCOPE

This policy applies to all individuals employed by or working under an employment contract with Your Chapter Holdings Limited. This includes Your Chapter Limited and Oasis Adolescent Services Limited which are subject to the same terms and conditions outlined herein.

This policy applies to all our staff.

This policy, which is part of our suite of data protection related policies, must be followed in conjunction with those other policies

This policy applies to all of our business activities that involve the processing of personal data.

DEFINITIONS

Data Protection Legislation means the UK General Data Protection Regulation, ('UK GDPR'), the Privacy and Electronic Communications Regulations ('PECR') and (where applicable) the EU General Data Protection Regulation ('EU GDPR').

Personal data (aka Personal Information and Personally Identifiable Information or PII) means any information relating to an identified or identifiable person ('Data Subject').

Personal data breach means a security incident that has affected the confidentiality, integrity, or availability of personal data (whether accidental or deliberate).

Examples of personal data breaches are:

- Theft or loss of devices containing personal data
- Inappropriately accessing files containing personal data about customers/staff
- Using customer personal data for personal benefit
- Sending an email to the wrong recipient by mistake

Data subject means any individual whose personal data is processed by us.

Processing means any use of personal data such as the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, dissemination, erasure and destruction. (This means that virtually anything we do with personal data will be 'processing').

Staff means **anyone working at or for** us including:

- Board members
- Directors
- Permanent, interim, and temporary employees and workers
- Consultants
- Contractors

PURPOSES

- To ensure all personal data is processed in accordance with Data Protection Legislation
- To respect the privacy of individuals
- To ensure personal data is processed by us in a consistent manner
- To reduce the risk of a personal data breach
- To provide guidance to staff about how to comply with Data Protection Legislation
- To clarify responsibilities and roles for implementing this policy and monitoring compliance with it.
- To clarify and facilitate our decision-making about whether or not to notify the ICO, any other regulators or organisations and any individuals about a personal data breach.

ROLES AND RESPONSIBILITIES

Our Senior Management team have ultimate responsibility for ensuring compliance with Data Protection Legislation and this policy.

The Data Protection Officer (DPO), has responsibility to

- Remind the Senior Management team of their responsibility for ensuring our compliance with Data Protection Legislation and this policy; and
- Advise the Senior Management team how to exercise their responsibility for ensuring our compliance with Data Protection Legislation and this policy; and
- Monitor our compliance with Data Protection Legislation and this policy

Our Data Protection Group (see Appendix) has responsibility to liaise with the DPO to help ensure we comply with the Data Protection Legislation and this policy.

All staff have a responsibility to comply with Data Protection Legislation and this policy when carrying out their duties.

Line managers are responsible for ensuring staff's adherence with this policy.

Failure to comply with this policy may result in legal and/or disciplinary action.

ABOUT PERSONAL DATA BREACHES

Personal data breaches can happen for a wide range of reasons, for example:

- Human error
- Cyber-attacks (e.g., hacking, phishing, social engineering)

Examples of the potential consequences of a personal data breach to us are:

- Fines and/or other penalties from regulators
- Commercial detriment, including loss of business value
- Loss of reputation
- Disruption to our business

- Claims for compensation

Examples of the potential consequences of a personal data breach to our data subjects are:

- Breach of privacy
- Inability to access their data
- Harms, including stress, financial loss and identity theft
- Disruption to their business and/or life

PROCEDURE FOR DEALING WITH PERSONAL DATA BREACHES

All Staff must, as a matter of urgency, report a suspected or identified personal data breach to our Data Protection Group.

Our Data Protection Group must contact our DPO as a matter of urgency.

Our DPO will decide if a personal data breach has occurred.

If our DPO advises that a personal data breach has occurred, he/she will, if instructed to do so, be responsible for instigating and supporting an investigation which will primarily focus on the following key considerations:

1. Containment and recovery
2. Assessment of risks
3. Deciding whether to notify the Information Commissioner's Office (ICO), and/or any individuals and/or any third parties
4. Evaluation and response

The investigation team, will comprise, in addition to our DPO, all or any of the following:

- A member of the Board
- The CEO
- One or more Directors
- One or more members of the Data Protection Group
- The Heads of IT/HR/Marketing/PR/Finance

ORGANISATIONAL MANAGEMENT OF PERSONAL DATA BREACHES

The DPO will keep a log of all suspected or identified personal data breaches reported, to allow any trends to be identified and addressed.

The Head of Human Resources will consider whether disciplinary action should be taken against any member of staff who has not complied with this policy.

The Senior Management team will consider whether legal action should be taken against any third party who has caused or contributed to a personal data breach for which we have a responsibility under Data Protection Legislation.

Appendix

At the time this policy was last updated, the members of our Data Protection Group were:

1. Ian Oatley, Finance Director, Ian.Oatley@yourchapter.co.uk.
2. Paul Robinson, Operations Director, paul.robinson@yourchapter.co.uk

This policy was last updated on **20/11/2024**