Lower Covey Ltd
Established 1929
Chapel Lane, Yetminster, Sherborne, Dorset, DT9 6LJ
01935 422215 info@lowercovey.co.uk

Lower Covey Montessori Nursery

Pear Tree Nursery & Pre-school

October 2021

Data Breach Policy

Introduction

Lower Covey Ltd holds and processes personal data. Every care is taken to protect such data from incidents (either accidental or deliberate) which may result in a data protection breach that could compromise security. We recognise that any compromising of the information we hold, whether in terms of breach of confidentiality, integrity or availability, may result in harm to individual(s), reputational damage and/or have a detrimental effect on service provision. It may also amount to legislative non-compliance and/or result in financial costs.

Objective

Our objective is to contain any breaches, to minimise the risk associated if a breach does occur and to consider what action is necessary to secure the relevant data and prevent such further incidents.

Purpose of the Policy

This policy recognises the duty imposed by the General Data Protection Regulation (GDPR) to report certain types of personal data breach to the relevant supervisory authority (the Information Commissioner's Office (ICO)) within 72 hours of becoming aware of the incident. It sets out how we plan to prevent such a breach, the steps we will take if it nevertheless becomes apparent that one has occurred, and the responsibilities of various members of staff within this process.

Scope of the Policy

This policy relates to all personal and special categories of data (including commercially sensitive information) held by Lower Covey Ltd regardless of format. It applies to all staff including temporary, casual or agency workers and contractors, consultants, suppliers and data processors working for, or on behalf of the organisation.

Personal Data

Under the GDPR, personal data is "any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

Identifying a 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 as it can include:

- access by an unauthorised third party
- attacks on a website
- deliberate or accidental action (or inaction) by a controller or processor
- sending personal data to an incorrect recipient
- computing devices (laptops, USB sticks, etc) or paper records containing personal data being lost or stolen
- accidental destruction of such equipment or files in a fire or flood
- “blagging” offences where information is obtained by deceiving the organisation which holds it
- alteration of personal data without permission
- loss of availability of personal data.

In the context of the above examples, Lower Covey Ltd recognises that there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware.

Responsibilities

While there is a corporate responsibility to ensure that all data is processed in accordance with the GDPR and other relevant legislation, including the Data Protection Act 2018, certain members of the organisation have particular responsibilities in the event of a data breach. All persons covered by the scope of this policy are responsible for reporting actual, suspected, threatened or potential data breaches and for assisting with investigations as required, particularly if urgent action must be taken to prevent any or further damage.

However, the Data Protection Officer (DPO) Shellie Prager, must be involved at the earliest opportunity and will be initially responsible for calculating the extent of the breach.

Training

The steps to be taken in the event of an actual or suspected breach, including the immediate necessity of informing the DPO or the nominated person, must be included in any introductory briefing on information management and security procedures delivered to all new staff. It must be made clear at this early stage that failure to comply with these requirements may result in disciplinary action.

When A Breach Is Discovered

It is the responsibility of whoever discovers a breach, or potential breach, to collect full details (including dates and times) and, if known, the type of data and the number of data subjects involved. This information must be

passed immediately, or, if the breach is discovered outside normal working hours, as soon as possible, to the DPO or the person responsible for data protection in the organisation

Initial Action to be Taken

Either the DPO, or the person responsible for data protection, must then take the following actions.

- Ascertain if the problem is still ongoing and, if so, take the necessary steps to stop the breach from continuing.
- Make an initial assessment of the extent of the breach.
- Decide, in consultation with the organisation's management, who will carry out further investigation of the causes and likely impact of the incident.
- Decide if it is of a level of seriousness that requires notification to the ICO (is there a risk to people's rights and freedoms?) or the police (has the data been compromised/stolen by a criminal act?).
- Establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

[Note: If it is decided that the breach is not of a level of seriousness that would require it to be reported, Lower Covey Ltd will document and retain any evidence which justified this decision.]

Risk Assessment

The person responsible for carrying out the investigation into a data breach will, within the first 24 hours (if possible), carry out an initial assessment of the extent of potential harm. This will focus on:

- the type of data involved and its level of sensitivity
- the volume of data stolen, copied or compromised
- the number of data subjects involved (that is, the persons affected or likely to be affected)
- the individuals/organisations that carried out the breach (if known)
- the extent to which the files involved were encrypted or password-protected.

Information to be Supplied

If it is decided that a serious breach has occurred that must be reported to the ICO, the following information will be made available.

- A description of the nature of the personal data breach including, where possible, the categories and approximate number of individuals concerned.
- The categories and approximate number of personal data records concerned.
- The name and contact details of the DPO or the person chosen to liaise with the authorities.
- A description of the likely consequences of the personal data breach
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

[Note: It is accepted that organisations may not be able to carry out all the necessary checks, or to supply all the required information, within the laid-down 72-hour period. It is important, however, that initial contact is made within that period, even if it is only to explain why there will be a delay in supplying full details. In this event, the organisation should emphasise that it has made dealing with the breach a priority and is devoting all possible resources to the investigation. If in doubt, call the ICO helpline: 0303 123 1113.]

Levels of Seriousness

When deciding whether a breach is sufficiently serious to be notified to the ICO, the following points should be borne in mind.

- Is there a high risk of it adversely affecting the rights of data subjects?
- Would notification enable them or others on their behalf to take mitigating action?
- Would notification help to prevent the unauthorised or unlawful use of the data concerned?
- Does this organisation have a contractual duty to take such action?

[Note: Not all breaches will merit being reported to the authorities, but in all cases the persons affected should be informed of how and when the breach occurred, what has been done to correct the situation and what they may wish to do to further safeguard themselves. A contact within the organisation must be provided so that those affected have access to further information.]

Further Action

During the aftermath of a breach, in the reporting and investigation stages, the required information should not only be gathered and supplied as appropriate but should also be recorded. This should form the basis of a final report into the breach, to be prepared by the DPO or the person responsible for data protection, which will be considered at the highest level within the organisation (board, senior management, owner, etc).

This report should include recommendations for remedial action and improvements in the organisation's data protection policy as appropriate and should consider the need for further training of relevant staff.