Data Breach Policy

The General Data Protection Regulation (GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The GDPR places obligations on staff to report actual or suspected data breaches and our procedure for dealing with breaches is set out below. All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it.

This policy does not form part of any individual's terms and conditions of employment with the setting and is not intended to have contractual effect.

Personal Data

Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access.

Personal data can be factual (for examples a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.

Current measures in place to limit data breaches:

- Undo send activated on gmail
- Locked cabinet in office, restricted user drawers, office door locked when unmanned
- All paper waste shredded
- Laptops/ tablets/ smartphones password protected and changed when an employee leaves
- Staff aware of scam emails and advised not to open them

Data Breach Procedure

What is a personal data breach?

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.

Examples of a data breach could include the following (but are not exhaustive):

- Loss or theft of data or equipment on which data is stored, for example loss of a laptop or a paper file (this includes accidental loss)
- Inappropriate access controls allowing unauthorised use

- Human error (for example sending an email or SMS to the wrong recipient)
- Unforeseen circumstances such as a fire or flood
- Hacking, phishing and other "blagging" attacks where information is obtained by deceiving whoever holds it.

When does it need to be reported?

The Centre must notify the ICO of a data breach where it is likely to result in a risk to the rights and freedoms of individuals. This means that the breach needs to be more than just losing personal data and if unaddressed the breach is likely to have a significant detrimental effect on individuals.

Examples of where the breach may have a significant effect includes: -

- Potential or actual discrimination;
- Potential or actual financial loss
- Potential or actual loss of confidentiality
- Risk to physical safety or reputation
- Exposure to identity theft (for example through the release of non-public identifiers such as passport details)

If the breach is likely to result in a high risk to the rights and freedoms of individuals then the individuals must also be notified directly.

Reporting a data breach

If you know or suspect a personal data breach has occurred or may occur which meets the criteria above, you should:

Discuss with the Office Manager who will take appropriate steps to deal with the report in collaboration with the DPO.

Preventing Future Breaches

Once the data breach has been dealt with, the centre will consider its security processes with the aim of preventing further breaches.

Reviewed by: Sue Erickson
Reviewed date: Jan 2019
Next review: Jan 2020

Endorsement:
Full endorsement of this policy is given by:

Stuart Brown
Rose Garden Early Years Centre Director

Signed: 

Dated: 7th February 2019