1st Goostrey Scout Hut
220 Main Road
Goostrey
Cheshire CW4 8PE

Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO and should be used in conjunction with the Pre-Schools Data Protection Policy.

On finding or causing a breach, or potential breach, the Pre-School manager or data processor must immediately notify the DPO. The Pre-School manager will ask the member of staff to record the breach in a confidential book.

The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people

The DPO will alert the Pre-School manager and the Committee chair

The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)

The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen

The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

- Loss of control over their data
- Discrimination
- Identify theft or fraud
- Financial loss
- Unauthorised reversal of pseudonymisation (for example, key-coding)
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

The DPO will document the decision (either way) in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored within the record of data breaches.

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out 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
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts and cause
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored as a hard copy within the Pre-Schools storage facility

The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being lost:

- All electronic devices including laptops, tablets, USB memory sticks are encrypted and password protected.
- Where it is necessary to take paper records and/or electronic files/devices offsite all staff understand they are responsible to ensure that they will never be left unlocked and/or unattended in a car, public place or place where they could easily be stolen.
- Staff are aware of the importance of putting paper records and/or electronic devices back at the end of the day. them to the caretaker so that he can lock them away.

Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error, requesting the sender recall the message

In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way

The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request

The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Website:

Whilst our website has been designed and is hosted by CBJ Digital Ltd, we have full control over all of the information that is published. Therefore, if there was a case where certain data was published inappropriately, it could be taken down immediately.

Contracts with third parties:

Within Pre-School we have contract with a number of organisations to support us in running the Pre-School more efficiently. With each contract we have it in writing that they follow and implement all of the necessary procedures linked with GDPR and therefore if they have their own data breach, they would also be committed to following the appropriate procedures.