PERSONAL DATA BREACH POLICY AND PROCEDURES

Policy Number 9.9

Policy Statement

Churchwood Kindergarten processes personal data, including special category personal data. It is essential that procedures are in place to ensure any threat to the security of that information is minimised, and any breaches of the duties in respect of that information are identified and remedied. Any incident that compromises the security of that information, or the system in which it resides, must be managed appropriately and in accordance with legislation and guidance provided by the Information Commissioner's Office (ICO).

The purpose of this policy is to ensure that Churchwood Kindergarten reacts appropriately to mitigate the risks associated with actual or suspected security incidents relating to information systems and data. Churchwood Kindergarten recognises that there are risks associated with users accessing and handling information to conduct kindergarten business. This policy aims to mitigate the following risks:

- Reduce the impact of information security incidents by ensuring they are followed up correctly.
- Improve compliance by ensuring serious security incidents are reported to the appropriate external organisations.
- Help identify areas for improvement to decrease the risk and impact of future incidents.

Churchwood Kindergarten is required to keep a record of all security incidents involving personal data. Some of these incidents must be reported to the Information Commissioner within 72 hours of detection, and without undue delay to individuals affected by the incident.

Definitions

Personal data

Personal data, or personal information, is defined as any information that relates to an identified or identifiable living individual. Different pieces of information which, when collected together, can lead to the identification of a particular person also constitute personal data/information.

Special category data

Special category data is personal data which the General Data Protection Regulation (GDPR) says is more sensitive, and so needs more protection. For example, it is information about an individual's:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or

- sexual orientation.

In particular, this type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination.

Classifications

A personal data breach is more than just losing personal data. It is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This policy needs to be applied as soon as information systems or data are suspected to be, or are actually affected by, an adverse event which is likely to lead to a security incident.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data.
In short, 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, or accidentally lost or destroyed.

Examples of the most common personal data breaches and information security incidents are listed below. It should be noted that this list is not exhaustive:

- Giving information to someone who should not have access to it – this could be verbally, in writing, or electronically.
- Theft or loss of a confidential paper.
- Sending personal data to an incorrect recipient.
- Sending a text message containing personal data to all parents by mistake.
- Writing down your password and leaving it on display or somewhere easy to find.
- Printing or copying confidential information and not storying it correctly or confidentially.
- Safeguarding information being made available to an unauthorised person.
- Computer becoming infected by a virus or other malware.
- Finding data that has been changed by an unauthorised person.
- Use of unapproved or unlicensed software on kindergarten ICT equipment.
- Accessing information using someone else's authorisation (eg: someone else's user ID and password).
- Changes to information, data, or system hardware, firmware or software characteristics without the Director's knowledge, instruction or consent.
- Unwanted disruption or denial of service to a system.
- Unauthorised use of a system for the processing or storage of data by any person.

Handling procedure

- If a personal data breach has is known to have occurred, or is suspected to have occurred, staff should not attempt to investigate the matter themselves.
- Staff should immediately contact the Data Protection Officer (DPO) who is the person designated as the key point of contact for personal data breaches. The kindergarten's DPO is Emma Draper.
- All evidence relating to the potential personal data breach should be preserved.

- On finding or causing a breach, or potential breach, the DPO must take immediate steps to mitigate and remedy the breach that has occurred.
- All reasonable steps must be taken to retrieve any information that has been unlawfully disclosed.
- The DPO will provide advice on the immediate steps to be taken, investigate the report, and determine whether a breach has occurred.
- The DPO will assist relevant members of staff, or data processors, where necessary to mitigate risk and impact.
- The actions to be taken will be relevant to specific data types.
- The actions to minimise the impact of data breaches are set out below. These must, where relevant, be taken to mitigate the impact of different types of data breach.
- The DPO will review the effectiveness of these actions and amend them as necessary after any data breach.

Investigation and report

- The DPO will carry out an internet search to check that the information has not been made public.
    - If it has, the DPO will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.
- The DPO will assess the potential consequences, based on how serious they are and how likely they are to happen.
- The DPO will assess 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, or cause them any physical, material or non-material damage (eg: emotional distress), including through:
    - loss of control over their data;
    - discrimination;
    - identity theft or fraud;
    - financial loss;
    - unauthorised reversal of pseudonymisation (for example, key-coding);
    - damage to reputation;
    - loss of confidentiality; and

- any other significant economic or social disadvantage to the individual(s) concerned.

- If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO within 72 hours of the personal data breach coming to their attention.
- 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.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website.
- 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; and
    - 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.

Recording

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 causes.
- The effects.
- The action to be 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 securely on the kindergarten's systems.

Review and planning

The DPO and kindergarten staff will meet to review what happened and how it could be prevented from happening again. This meeting will happen as soon as is reasonably possible after the event.

Reporting information security weaknesses

- Security weaknesses, for example a software malfunction, must be reported through the same processes as security events.
- Users must not attempt to prove a security weakness as such action may be considered to be a misuse of information assets.
- Weaknesses reported to third party application and service providers by users must also be reported internally to the DPO.
- The provider's response must be monitored and the effectiveness of its action to repair the weakness must be recorded and reported.

Security events can include:

- Uncontrolled system changes.
- Access violations – eg: password sharing.
- Breaches of physical security.
- Non-compliance with policies.
- Repeated lock out of user accounts.
- Flooding of the system with emails.
- Malicious software (virus infections).
- Unscheduled shutdowns, system errors or overloads.

Security weaknesses can include:

- Inadequate firewall or antivirus protection.
- System malfunctions or overloads.
- Malfunctions of software applications.
- Human error.

All events must be reported to the DPO. A risk impact assessment must be carried out and mitigation action, including implementation time frames, identified.

Policy Monitoring and Review

This policy is monitored by the staff and management of Churchwood Kindergarten and will be reviewed annually, or before if necessary.

Date created: 7th September 2019
Created by: Caroline Bennetts
Reviewed by:
Signed: …… *Date: ……*
Name: …….. *Role: ……*

Review date: 7th September 2020
Reviewed by:
Amended / Updated? *Yes / No*
Brief explanation of changes:

Signature of reviewee:
New review date set: