LINKS CHILDCARE POLICIES & PROCEDURES		
GDPR POLICY **DATA BREACH HANDLING PROCEDURE**		
Last Review Date: June 2023	Policy No.56 B	Issued: 2018

What is a Data Breach?

A data breach is an incident in which personal data held by Links Childcare on staff or families has been lost, accessed, and/or disclosed in an unauthorised fashion.

This would include, for instance, loss or theft of a laptop containing personal data, an email with personal information being sent to the wrong recipient, loss of paper files or records containing personal data, as well as more organised incidents of external hacking.

The purpose of the Data Breach procedure is to ensure all necessary steps are taken to:

(i) Contain the breach and prevent further loss of data

(ii) Ensure data subjects affected are advised (where necessary)

(iii) Comply with the law on reporting the incident to the Data Protection Commissioner if necessary

(iv) Learn from the incident - identify what measures can and should be put into place to prevent similar occurrences in the future

Data Breach Response Plan – what we will do

- Nominate Breach Incident Manager and designate formal point of contact.
- Identify Stakeholders
- Set up breach response handling team - can comprise of the Manager / Support Staff / external IT supplier / partner representatives / third party representatives as deemed necessary
- Work systematically through six-step process below, evaluating key steps required and critical outcomes at each stage

The Need to Inform Data Subjects

"Data controllers who have experienced an incident giving rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data must give immediate consideration to notifying the affected data subjects. As the Code states, "this permits data subjects to consider the consequences for each of them individually and to take appropriate measures." The consequences may include the

potential for fraud / identity theft, but it may also involve the potential for damage to reputation, public humiliation or even threats to physical safety." (extract from the DPC Guidance on Breach Notification)

The information communicated to data subjects will include information on the nature of the personal data breach and a contact point where more information can be obtained. It should recommend measures to mitigate the possible adverse effects of the personal data breach.

The Need to Inform the Office of the Data Protection Commissioner (DPC)

" .. the Code of Practice states that ***all incidents in which personal data has been put at risk should be reported to the Office of the Data Protection Commissioner.*** *The only exceptions are when the data subjects have already been informed* ***and*** *the loss affects no more than 100 data subjects* ***and*** *the loss involves only non-sensitive, non-financial personal data. The Code also makes clear that if a doubt exists - especially whether the technological measures protecting the data are such as to permit a reasonable conclusion that the personal data has not been put at risk - the matter should be reported to the Office of the Data Protection Commissioner."* (extract from the DPC Guidance on Breach Notification)

Complex personal data security breach incidents may take a considerable period to fully investigate and resolve. The initial contact with the Office should be limited to describing the facts as they are known and the steps being taken to address those facts. The personal data involved should not be included in such reports to the Office of the Data Protection Commissioner.

Responsibility for Communication of Breach

In the event of a data breach, it is the responsibility of the Designated Person to determine which notifications are necessary and to ensure they take place without delay. The maximum timeframe for notification to the Office of the Data Protection Commissioner has been set at 72 hours from the time the incident is first discovered.

Data Breach - Six Step Process

1. **Identification and Confirmation:** Identify and confirm volumes and types of data affected, and all data subjects/members involved.
2. **Containment - typically:**
    a. Identify source of breach
    b. Limit scope of negative impact
    c. Isolate - database/network/mobile devices
    d. Denial of login access
    e. Partial or complete systems lockdown
3. **Analysis**: Detailed analysis of volumes and types of data involved & identify gateways/source/location and cause of data loss.
4. **Notification of DPC / Data Subjects / Other:** Timing is critical. Consider need to inform:
    a. Data subjects, whether notification is urgent and/or necessary need for further action on their part (change passwords, notify banks/ etc)
    b. Supervisory Authority i.e. Office of the DPC (within 72 hours of first becoming aware of the breach)
    c. Other third-party stakeholders
5. **Damage Control**: In the event of major breach:
    a. Advise and involve highest level of management / partner / public body representatives.
    b. Have a communication plan in place for Data Subjects, Regulators, Public Bodies, Press, etc.
    c. Channel all communication through a single source e.g. coordinated press-releases.
    d. Review all third-party contracts - be aware of your responsibilities and liabilities.
6. **Lessons Learned**
    a. Conduct thorough lessons learned exercise.
    b. Improve processes to avoid future data breaches.
    c. Consider independent/third-party audit to review your organisation's policies and compliance efforts, as well as its technical infrastructure.

Review Dates:	June 2023		