Yeading

YEADING INFANT & NURSERY SCHOOL

DATA BREACH POLICY

Policy Statement

Yeading Infant & Nursery holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the unlikely event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This breach procedure applies to all personal and sensitive data held by Yeading Infant & Nursery. This procedure applies to all school staff including governing bodies, referred to herein after as 'staff'.

Purpose

This breach procedure sets out the course of action to be followed by all staff at Yeading Infant & Nursery if a data protection breach takes place.

Introduction

Data Protection legislation is changing May 2018. The Data Protection Act 1998 will be superceded by the EU General Data Protection Regulation (GDPR).

GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified.

All Organisations are legally required to ensure any Personal Data is processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. It requires that appropriate technical or organisational measures are used.

GDPR places a duty on all Organisations to manage, report (where necessary), and investigate all personal data breaches.

Types of Breach

Under GDPR, 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.

Data protection breaches could be caused by a number of factors. Some examples are:

- Loss or theft of pupil, staff or governing body data and/ or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment Failure
- Human Error
- Unforeseen circumstances such as fire or flood
- Hacking
- "Blagging" offences where information is obtained by deception.

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 and this unavailability has a significant negative effect on individuals.

Recital 87 of the GDPR makes clear that when a security incident takes place, you should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it. This includes notifying, where required, the appropriate Supervisory Authority. In the UK, this role is held by the Information Commissioners Office (ICO).

Immediate Containment/Recovery

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. You must do this **within 72 hours of becoming aware** of the breach, where feasible.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.

In discovery of a data protection breach, the following steps should be followed:

1. The person who discovers/receives a report of a breach must inform the Head Teacher or, in their absence, either the Deputy Head Teacher or the School Business Manager. If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.

2. The Data Protection Officer (DPO) should be informed as soon as is practicable (within 24 hours of the breach being detected).

3. The Head Teacher (or nominated representative) and DPO must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff such as the IT technician.

4. The Head Teacher (or nominated representative) should inform the Chair of Governors.

5. The Head Teacher (or nominated representative) and DPO must consider whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

6. The Head Teacher (or nominated representative) and DPO must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

    - Attempting to recover lost equipment.
    - Contacting the relevant Local Authority Departments, so that they are prepared for any potentially inappropriate enquiries ('phishing') for further information on the individual or individuals concerned. Consideration should be given to a global email to all school staff. If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer's name and contact details if possible and confirm that they will ring the individual making the enquiry back. Whatever the outcome of the call, it should be reported immediately to the Head Teacher (or nominated representative) and DPO.
    - The use of back-ups to restore lost/damaged/stolen data.
    - If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.
    - If the data breach includes any entry codes or IT system passwords, then these must be changed immediately, and the relevant agencies and members of staff informed.

Investigation

In most cases, the next stage would be for the Head Teacher (or nominated representative) and DPO to fully investigate the breach. This should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation should consider:

- The type of data
- Its sensitivity
- What protections are in place (e.g. encryption);
- What has happened to the data;
- Whether the data could be put to any illegal or inappropriate use
- How many people are affected
- What type of people have been affected (pupils, staff members, suppliers etc) and whether there are wider consequences to the breach.

A clear record should be made of the nature of the breach and the actions taken to mitigate it. This should be added to the School's breach register.

The investigation should be completed as a matter of urgency and, wherever possible, within 5 days of the breach being discovered/reported. A further review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

Notification

Where a breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must notify the ICO within 72 hours of the breach being detected.

The school must also contact the individuals affected within 72 hours.

In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals. Recital 85 of the GDPR explains that:

"A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised.

It is essential that the School with assistance from their DPO, assess this case by case, looking at all relevant factors.

If the school is unsure whether an incident should be notified to the ICO they should immediately contact their DPO for advice.

Review and Evaluation

Once the initial aftermath of the breach is over, the Head Teacher (or nominated representative) and DPO should fully review both the causes of the breach and the effectiveness of the response to it.

It should be formally documented and made available to the Senior Leadership Team (SLT) for discussion.

If systemic or ongoing problems are identified, then an action plan must be drawn up to address those problems. If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with Human Resources for advice and guidance.

This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance. Consideration should be given to reviewing this breach procedure whenever the data protection policy is reviewed.

Implementation

The Head teacher should ensure that all staff are aware of the Data Protection policy and its requirements including this breach procedure. This should be undertaken as part of induction and supervision.

If staff have any queries in relation to the policy, they should discuss this with their line manager or the Head Teacher.

Signed by Chair of Governors..... **Date**.....24/5/18.....