Breach Reporting Policy

Our Lady and St Joseph Catholic Primary School

Prepared by: P Devereux
Approved by: Governing Body
Date: March 2018
Review Date: March 2021
Checked DPO: March 2018

BREACH REPORTING POLICY

'With Christ at our centre, we love, listen and learn'

Purpose of the Policy

To ensure that:

- Data breach events are detected, reported, categorised and monitored consistently
- Incidents are assessed and responded to appropriately
- Action is taken to reduce the impact of disclosure
- Mitigation improvements are made and put in place to prevent recurrence
- Serious breaches are reported to the ICO
- Lessons learnt are communicated within OLSJ and to external organisation as appropriate and work is carried out to prevent future incidents

Aims

- To ensure all breaches are reported clearly, and consistently. To document the circumstances of the breach, what actions are to be taken, what recommendations have been made and whether disciplinary action process needs to be followed
- To identify what actions need to be taken to first prevent a recurrence of the incident and second to determine whether the incident needs to be reported to the ICO
- To prevent further incidents, and focus on trends and improvements to reduce the likelihood and impact of recurrence

Definition

A Data Protection breach is the result of an event or series of events where personal and/or sensitive data is exposed to unauthorised or inappropriate processing that results in it's security being compromised. The extent of damage or potential damage caused will be determined by the volume, sensitivity and exposure of the information.

Examples of common incidents

Type	***Example***
Technical	Data Corruption Corrupt Code Hacking
Physical	Unauthoried/unescorted visitors on premises Break-ins to site Thefts from site Thefts from unsecured site Loss in transit/post
Human Resources	Data Input errors Non-secure disposal of hardware or paperwork Unauthorised disclosures Use of incorrect fax numbers/email addresses Inappropriate sharing

Responsibilities

All staff members have a responsibility to report a breach of conduct, however minor. The Data Protection Officer will ensure that the breach is investigated and the correct process followed, to ensure further incidents are prevented. All staff have a role to play to ensure a safe and secure workplace. All policies require the participation of staff and contractors to be successful. Any employee or contractor found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

All breaches are to be reported on the attached form, and handed to the Data Protection Officer for review.

OLSJ
OUR LADY + ST JOSEPH
CATHOLIC PRIMARY SCHOOL

Data Protection Breach reporting Form

1. Summary of Incident

Date and Time of Incident:	
Number of people whose data is affected:	
Department:	
Nature of breach: **e.g. Theft/disclosed in error/technical problem**	
Description of how breach occurred:	

2. Reporting

When was breach reported?	
How did you become aware of the breach?	
Has DPC and DPO been informed? **DPC – Patrick Devereux** **DPO – Lucy Henderson/Louise Manthorpe**	

Sections 3 to 6 are to be completed by DPC/DPO

3. Personal Data

Full description of personal data involved (without Identifiers);	
Number of individuals affected:	
Have all affected individuals been informed?	
If not, state why not:	
Is there any evidence to date that the personal data involved in this incident has been inappropriately	

processed or further disclosed? If so, please provide details:	

4. Data Retrieval

What immediate remedial action was taken:	
Has the data been retrieved or deleted? If yes – date and time:	

5. Impact

Describe the risk of harm to the individual as a result of this incident:	
Describe the risk of identity fraud as a result of this incident:	
Have you received a formal complaint from any individual affected by this breach? If yes, provide details:	

6. Management

Has the employee(s) involved breached policies and procedures?	
Has disciplinary action been taken in relation to the employee(s) involved?	
Had the employee(s) completed GDPR training?	**YES/NO**
As a result of this incident, do you consider whether any other personal data held may be exposed to similar vulnerabilities? If so, what steps have been taken to address this:	
Has there been any media coverage if the incident? If so, please provide details:	
What further action has been taken to minimise the possibility	

of a repeat of such an incident? Please provide copies of any internal correspondence regarding any changes in procedure:	