DATA BREACH PROCESS – OLIVER'S BATTERY PRIMARY SCHOOL

The GDPR requires that some, but not all data breaches must be reported to the ICO and in some cases the affected individual:

* Reporting to the ICO is required where a breach is likely to result in a risk to the rights and freedoms of individuals.

* Reporting a breach to the individual is required where it is likely to result in a high risk to their rights and freedoms.

A reportable risk exists when the breach may lead to damage to the individuals whose data have been breached. Examples of damage may include (but are not limited to) discrimination, identity theft or fraud, financial loss and damage to reputation. When the breach involves Special Category Data you should assume such damage is likely.

1.0 What to do if a breach is detected:

Report to the schools Data Protection Officer – Simon Sleeman, School Business Manager, who will then report to the Head Teacher and Governors to take appropriate action.

2.0 Contain, manage and recover the data breach

As soon as it becomes aware of a breach, the school must seek to contain the incident. Where possible recover the data breach.

3.0 Assess the data breach risk

Assess the risk that could result from it.

Taking into account the specific circumstances of the breach, think about the likelihood of the individual's privacy being impacted by the breach and what that impact might be.

Your assessment should always be objective, taking into account the following criteria:-.

3.1 The type of breach

This may affect the level of risk to individuals. For example, a breach where medical information has been disclosed to unauthorised parties has different consequences to a breach where an individual's medical details have been deleted and are no longer available.

3.2 The nature, sensitivity, and volume of personal data

Usually, the more sensitive the data, the higher the risk of harm will be to the people affected, but you should also consider the context. E.g the disclosure of the name and address of an individual would not generally cause substantial damage. But, disclosing the name and address of an adoptive parent to a birth parent could have significant consequences for the adoptive parent and child.

3.3 Ease of identification of individuals

Consider how easy it will be for a person who has access to the personal data to identify specific individuals, or match it with other information to identify individuals.

Personal data protected by an appropriate level of encryption will be unintelligible to unauthorised persons without the decryption key. Pseudonymisation can reduce the likelihood of individuals being identified in the event of a breach. This could be as simple as using Child A and Child B instead of names, while keeping a separate record of who it relates to

3.4 Severity of consequences for individuals

Depending on the nature and consequences of the personal data involved in a breach (e.g. Special categories of data) the potential damage to individuals could be very severe and could lead to identity theft, fraud, physical harm, Psychological distress, humiliation or damage to reputation. Breaches of the personal data of children could place them at particular risk of harm.

3.5 Special characteristics of the individual

A breach may affect personal data of children or other vulnerable individuals, who may be placed at greater risk of danger as a result.

3.6 The number of affected individuals

Generally, the higher the number of individuals the greater the impact a breach can have. A breach can however have a severe impact on even one individual, depending on the nature and context of the personal data involved.

We notify individuals where we deem the risk to be high to the individual. Please find below the information we must provide to individuals when telling them about a breach:

3.1 The name contact details of the DPO
3.2 A description of the likely consequences of the personal data breach and
3.3 A description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

4.0 Notify ICO where appropriate – You must do this within 72 hours of becoming aware of the breach, where feasible.

Where the consequences of a breach are more severe, the risk of damage is higher. If in doubt, the school should err on the side of caution and notify the ICO and, where relevant, the individual.
When reporting a breach, the GDPR states you must provide the following information:

4.1 A description of the nature of the personal data breach including, where possible:
4.2 The categories and approximate number of individuals concerned and the categories and approximate number of personal data records concerned
4.3 The name and contact details of the DPO
4.4 A description of the likely consequences of the personal data breach and
4.5 A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

5.0 Record Keeping
How should we document the breach?
Whether you report a breach to the ICO or not, you must keep records of all data breaches – The records should include:-

* What was the breach;

* What caused the breach;

* What personal data was affected;

* What the effects and consequences of the breach were;

* What remedial action was taken by the school.

You should also record the reasons for decisions taken in response to a breach, particularly, if a breach is not notified to the ICO.

If a notification to the ICO is delayed the school must be able to provide reasons for the delay and it will help if you have written evidence of this.

If you tell an affected individual about a breach you should do so in a clear, effective and timely manner and keep a record of the letter/email sent.