DATA SECURITY BREACH MANAGEMENT

Committee Responsible:	HR and Remuneration
Person Responsible:	Headteacher
Date Approved by FGB:	April 2018
Date for Review:	April 2019

Signed……..

Date……..

Introduction

The School's security measures seek to ensure that:

- only authorised people can access, alter, disclose or destroy personal data;
- those people only act within the scope of their authority; and
- if personal data is accidentally lost, altered or destroyed, it can be recovered to prevent any damage or distress to the individuals concerned.

All members of staff are expected to follow the Data Security Breach Process because breaches should be responded to swiftly and effectively.

The aim of this document is to ensure the appropriate course of action is taken in the event of a data security breach.

Procedures

1. Any and all breaches of the GDPR, including a breach of any of the data protection principles shall be reported as soon as it is discovered, to the Data Protection Officer (DPO) and to the Headteacher.

2. Once notified, the DPO will assess:

   - the extent of the breach;
   - the risks to the data subjects as a consequence of the breach;
   - any security measures in place that will protect the information and
   - any measures that can be taken immediately to mitigate the risk to the individuals. For example this could be recalling a mis-sent email, arranging for staff to recover documents etc.

3. An assessment of the ongoing risk will be made. Not all incidents result in potential adverse consequences to the individual whose data is compromised.

4. Unless the School concludes that there is unlikely to be any risk to individuals from the breach, it must be notified to the Information Commissioner's Office within 72 hours of the breach having come to the attention of the School.

5. Reporting of all breaches is not mandatory. Notification to both the individual concerned and the ICO is only required where there is a high risk of harm in terms of emotional distress, physical harm, financial damage or identity fraud.

6. Where the breach results in significant actual or potential detriment it should be reported to the ICO. Where a decision is made to report a breach to the ICO the notification should be made within 72 hours after

becoming aware of the breach. If made later the notification should explain the reason for the delay.

7. Notification to the Individual(s)

There are prescribed requirements for the notification to the individual therefore it is recommended that the precedent letter is used below. Notification is not required unless the risk to the individual whose personal data is involved is high. The risk could be in relation to identity fraud and/or serious harm. The draft notification anticipates failure to recover data and that there is a risk of serious harm.

Dear

I write further to our telephone conversation to advise you that there has been a data security breach in relation to your personal data being processed by the School.

The School takes very seriously it's responsibly to ensure personal data is processed fairly and lawfully and I offer the School's sincere apologies for what has happened. If there is anything that I can do to assist with managing the risks involved or to provide you with more information please contact me on [contact details].

The following data was involved [describe the biographical data about the individual e.g. full name, address, dob, health/financial details]

The breach was discovered on [date] and took place on [date] when [briefly describe how the breach occurred]

In accordance with our data security breach management processes and in line with ICO guidance we took immediate steps to respond to the risks posed by the breach. Unfortunately we were unable to contain and recover the information.

What steps the person can take to protect themselves [describe steps]

As part of our data security management process we will be undertaking a further evaluation with a view to establishing whether there are any steps we can take to improve security and minimise the risk of such a breach recurring.

8. Notification to the ICO

Serious breaches should be notified to the ICO using the ICO DPA Security Breach Notification Form which should be sent to the email address: casework@ico.gsi.gov.uk

Or by post to: Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

The ICO DPA Security Breach Notification Form is accessible on this link: https://ico.org.uk/for-organisations/report-a-breach/

The following information must be provided:

- date of breach and when detected.
- A description of the nature of the personal data breach (theft, loss, disclosed in error), the number of individual's data involved and the type and content of the records involved.
- name and contact details of the Data Protection Officer or other contact point.
- the likely consequences of the breach.
- the actions taken or proposed to be taken to contain or remedy the breach
- whether the individual has been notified.
- the reason for the delay if the notification is not made within 72 hours.

9. The School will then instigate an investigation into the breach, including how it happened, and whether it could have been prevented. Any recommendations for further training or a change in procedure shall be reviewed by the School and a decision made about implementation of those recommendations.
