Castle Newnham School

TRADITIONAL VALUES, BRIGHT FUTURES, ONE JOURNEY

Data Breach Management Procedure

Governors' Committee:	Resource Management Committee
Adopted by the Governing Body on:	22 January 2019
Signed: (Chair of Committee)	
Signed: (Headteacher)	
Proposed date of review:	January 2021

A. RATIONALE

As an organisation which processes personal data, every care is taken to protect personal data and to avoid a data protection breach. This policy outlines the measures our school takes against unauthorised or unlawful processing or disclosure and against accidental loss, destruction of or damage to personal data.

It is a regulatory requirement under GDPR for our school to have consistent and effective governance and control arrangements to protect the personal data that we hold. This Data Breach Procedure sets out the course of action to be followed by all staff in the event of a real or potential data protection breach.

B. AIM

The aim of this policy is to ensure a standardised and consistent approach is followed when responding to data breaches to enable us to:

1. report data breaches without delay to the Federation Principal and/or Data Protection Lead
2. Identify incidents of data breaches quickly and investigate them properly and in a timely manner
3. record and document all incidents and report them to the Senior Leadership Team (SLT), Governors and the Data Protection Lead(s)/DPO
4. asses the severity and impact of the data breach to determine whether it is necessary to inform the Data Subject(s) and ICO according to the GDPR guidance
5. take action which is proportionate, consistent and transparent to prevent further damage
6. regularly monitor and review all data breach incidents and potential situations that may lead to a data breach to identify improvements in policies, procedures and control mechanisms to remove or mitigate risk of further repetition

C. PRINCIPLES

In the event of data being lost or shared inappropriately, our school will take appropriate action to minimise any associated risk as soon as possible. This procedure applies to all personal and sensitive data held by **our school** and all school staff, Governors, volunteers and contractors, referred to herein after as 'staff'.

This Data Breach Procedure document forms part of the school's Data Protection Policy and all staff are made aware of these procedures through induction, supervision and ongoing training.

Definition of data breach

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.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In summary, 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, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Personal data breaches can include:

- Loss or theft of personal data and/or equipment on which data is stored
- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission;
- loss of availability of personal data
- hacking attack
- cyber attack
- equipment failure
- human error
- unforeseen circumstances such as a fire or flood
- flawed data destruction procedures

D. PROCESSES

1. Reporting a data breach

As soon as any member of staff, parent or governor discovers or receives a report of a data breach, they must inform the Federation Principal and/or the Data Protection Lead as soon as possible and without delay. If the breach occurs or is discovered outside normal school working hours, then notification should begin as soon as is practicable.

A verbal or emailed report can be submitted to the Federation Principal and/or Data Protection Lead in the first instance and should include accurate details of the incident.

An initial assessment of the data breach by the Federation Principal and/or Data Protection Lead will include completion of the Data Breach Incident Report Form to ascertain as much information as possible about the incident in order to fully assess the impact of the data breach and determine actions required.

2. Managing a data breach

Step 1: Containment and Recovery

1. The Federation Principal and/or Data Protection Lead will ascertain the severity of the breach, whether any personal data is involved and whether the breach is still occurring.

2. If the breach is still occurring, the Federation Principal and/or Data Protection Lead will establish what steps need to be taken immediately to minimise the effect of the breach and contain the breach from further data loss (e.g. alert the school's IT Technical support, restricting access to systems or close down a system etc).

3. The Federation Principal and/or Data Protection Lead will consider and implement appropriate steps required to recover any data loss where possible and limit damage caused (e.g. use of

backups to restore data; changing passwords etc.)

4. The Federation Principal and/or Data Protection Lead will inform the Chair of Governors if the severity and likely impact of the breach deems it necessary to inform the ICO of the breach. At the same time, depending on the nature of the breach, the Federation Principal and/or Data Protection Lead may seek expert or legal advice and/or the Police if it is believed that illegal activity has occurred or likely to occur.

5. Where a significant breach has occurred, the Federation Principal and/or Data Protection Lead will inform the ICO within 72 hours of the discovery of the breach (see Notifications below).

6. The decision taken as to the reasons why a data breach is either reported or not reported is documented by the Data Protection Lead.

7. All the key actions and decisions are fully documented and logged in our Data Security Breach Log.

Step 2: Assessment of Risk

Further actions may be needed beyond immediate containment of the data breach. To help the school determine the next course of action, an assessment of the risks associated with the breach is undertaken to identify whether any potential adverse consequences for individuals are likely to occur and the seriousness of these consequences.

The Federation Principal and/or Data Protection Lead will consider the points arising from the following questions:

1. What type and volume of data is involved?
2. How sensitive is the data? Could the data breach lead to distress, financial or even physical harm?
3. What events have led to the data breach? What has happened to the data?
4. Has the data been unofficially disclosed, lost or stolen? Were preventions in place to prevent access/misuse? (e.g. encryption)
5. How many individuals are affected by the data breach?
6. Who are the individuals whose data has been compromised?
7. What could the data tell a third party about the individual? Could it be misused regardless of what has happened to the data
8. What actual/potential harm could come to those individuals? E.g. physical safety; emotional wellbeing; reputation; finances; identity theft; one or more of these and other private aspects to their life
9. Are there wider consequences to consider?
10. Are there others that might advise on risks/courses of action (such as banks if individual's bank details have been affected by the breach)?

Step 3: Notification of breaches

If the severity and likely impact of the breach warrants notifying the ICO, then we will notify the ICO within 24 hours of becoming aware of the essential facts of the breach (through the ICO's online portal at https://report.ico.org.uk/security-breach/).

This notification will include at least:

1. our school name and contact details
2. the date and time of the breach (or an estimate)
3. the date and time we discovered it
4. basic information about the type of breach
5. basic information about the personal data concerned.

As we undertake a full investigation of the details of the breach, **within 3 days of the initial notification**, we will further provide the ICO with full details of the incident, the number of individuals affected and its possible effect on them, the measures taken to mitigate those effects, and information about our notification to the individuals affected.

There may be instances when the nature of the breach and the individual(s) affected may necessitate notifying third parties such as regulatory bodies, agencies, professional bodies as part of the initial containment.

If the breach is likely to adversely affect the personal data or privacy of our pupils, parents/carers, staff and/or governors, we will notify them of the breach without unnecessary delay if we cannot demonstrate that the data was encrypted (or made unintelligible by a similar security measure). We will inform them of:

- the estimated date of the breach
- a summary of the incident
- the nature and content of the personal data
- the likely effect on the individual(s)
- any measures we have taken to address the breach
- how those affected can mitigate any possible adverse impact

Step 4: Evaluation and response

When the school's response to a data breach has reached a conclusion, the Federation Principal and/or Data Protection Lead will undertake a full review of both the causes of the breach and the effectiveness of the response. The full review is reported to SLT and the Governing Board for information and discussion as soon as possible after the data breach has been identified.

If through the review, systematic or ongoing problems associated with weaknesses in internal processes or security measures have been identified as a cause of the data breach, then appropriate action plans will be drafted, actioned and monitored to rectify any issues and implement recommendations for improvements. The Governing Board will be party to discussions regarding action plans and be able to monitor progress against the actions appropriately.

If a breach warrants a disciplinary investigation, legal advice will be sought through Human resources channels.

E. MONITORING, ASSESSMENT & EVALUATION

The Federation Principal and/or Data Protection Lead will ensure that staff are aware of these procedures for reporting and managing data breaches. Data Protection training for all staff is mandatory, including new employees and all staff will undertake refresher training annually.

If staff have any queries or questions relating to these procedures, they should discuss this with the Federation Principal and/or Data Protection Lead.

Complaints about our Data Breach Management procedures

If an individual or Data Subject affected by a data breach believes that a data breach has not been dealt with properly, a complaint should be made to the school through our normal complaints procedure. If following the conclusion of the complaints procedure within the school, the individual or Data Subject is still dissatisfied, then a complaint can be made directly to the Information Commissioner's Office (ICO) at https://ico.org.uk/concerns .