Data Breach Policy Document

Rationale

Security breaches are increasingly common occurrences whether these are caused through human error or via malicious intent. As technology trends change and the creation of data and information grows, there are more emerging ways by which data can be breached. The School needs to have in place a robust and systematic process for responding to any reported data security breach, to ensure it can act responsibly and protect its information assets as far as possible.

The aim of this policy is to standardise the response to any reported data breach and ensure that they are appropriately logged and managed.

By adopting a standardised consistent approach to all reported incidents we aim to ensure that all incidents are reported in a timely manner and can be properly investigated using the following principals.

- incidents are handled by appropriately authorised and skilled personnel
- incidents are recorded and documented
- the impact of the incidents are understood and action is taken to prevent further damage
- evidence is gathered, recorded and maintained in a form that will withstand internal and external scrutiny
- external bodies or data subjects are informed as required
- the incidents are dealt with in a timely manner and normal operations restored quickly
- the incidents are reviewed to identify improvements in policies and procedures

Definition

A data security breach is considered to be "any loss of, or unauthorised access to, School, student or staff data". Examples of data security breaches may include:

- Loss or theft of data or equipment on which data is stored
- Unauthorised access to confidential or highly confidential School Data
- Human error
- Hacking attack
- where information is obtained by deceit

For the purposes of this policy data security breaches include both confirmed and suspected incidents.

Scope

This policy applies to all School information, regardless of format, and is applicable to all staff, students, visitors, contractors and data processors acting on behalf of the School.

All information users are responsible for reporting actual, suspected, threatened or potential information security incidents and for assisting with investigations as required, particularly if urgent action must be taken to prevent further damage.

SLT are responsible for ensuring that all staff in school act in compliance with this policy and assist with investigations as required.

DPO will be responsible for overseeing management of the breach in accordance with the Data Breach Management Procedure (below). Suitable delegation may be appropriate in some circumstances.

Data Classification

Data security breaches will vary in impact and risk depending on the content and the quantity of the data involved, therefore it is important that the School is able to quickly identify the classification of the data and respond to all reported incidents in a timely and thorough manner.

Public Data: Information intended for public use, or information which can be made public without any negative impact for the school.

Internal Data: Information regarding the day-to-day business and academic operations of the School. Primarily for staff and student use, though some information may be useful to third parties who work with the School.

Student Data: Information that is produced in school relating to a specific student, examples of this might be assessment data, personal information, health information or social status.

Staff Data: Information that is held in school usually in SIMS that is personal, examples of this might be address, medical information attendance information salary level etc.

Process document - Response to a data breach

This document is intended to provide guidance to SLT and staff around the actions that must follow a data breach in school.

The school must

- Detect, report and investigate personal data breaches
- Report any breach or potential breach to the DPO
- Assess and report any breaches to the ICO within 72 hours where the individual is likely to suffer some form of damage, e.g. through identity theft or a breach of confidentiality
- Communicate a breach to individuals concerned, where appropriate

When reporting a breach, you must set out the:

Date of Breach

You must set out the date of the breach and the date you were made aware of the breach. If there is a big difference between the dates you should also explain within the breach report why there is a discrepancy.

Nature of the Breach

Detail the circumstances which have led to the breach including how you become aware of the breach.

Data and individuals affected

What information was affected and how many people are affected by the breach (don't need to name people, just the number of people affected).

Effects of the Breach

This could be actual or potential effects (such as loss of confidentiality, breach of security). Detail the risk to the school as well as to the individuals affected.

Action Taken

Detail here any measures taken to remedy the breach (for example preventing the information from being disclosed to further parties, recalling documents, reporting the matter to the ICO, DPO or to the individuals directly). Include dates that these actions were taken.

Also include any steps you have taken to prevent future breaches.

Status

Finally to detail whether this action is completed (with what the last action was, for example matter closed by the ICO, matter closed by the leadership team as the matter didn't need to be reported).

ICO contact details Tel 030312311139

Policy to be Reviewed: January 2021