MEDINA HOUSE SCHOOL

DATA BREACH INCIDENT REPORTING POLICY

MAY 2019

Adopted by Governors ……

Signed by …… Chair of Governors

Created May 18, Reviewed: December 2018, May 2019

Review date: May 2020

Introduction

Medina House School holds large amounts of data including personal data relating to pupils and staff. The school is considered the data controller for all personal data that it processes, and, as such, it has responsibilities to ensure that all data is processed securely and in accordance with the requirements of relevant data protection legislation.

Every care is taken to protect personal data and to ensure that it is only shared with those who are entitled to access it. However, in the event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible.

This policy applies to all personal and sensitive data held by the school including all school information processed by staff, other professionals, volunteers and contractors. All staff are required to comply with the policy. Disciplinary action will be taken against staff who fail to ensure the safe and secure processing of personal data.

The Information Commissioners Office (ICO) has the power to take enforcement action against any organisation that breaches data protection legislation. Under the General Data Protection Regulation (GDPR), that came into effect in May 2018, these powers are extended to include the ability to impose fines of up to 4% of gross turnover or 20 million euros.

1. Purpose

This breach policy explains what a data breach is, and sets out the course of action to be followed by all staff if a data protection breach takes place.

2. Definition - What is a Personal Data Breach?

A "personal data breach" is defined as:

"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

A breach is a type of security incident. Whilst all personal data breaches are security incidents, not all security incidents are necessarily personal data breaches.

The consequence of a personal data breach is where the school is unable to ensure compliance with the data protection principles.

Breaches can be categorised according to the following principles:

- "Confidentiality breach" - where there is an unauthorised or accidental disclosure of, or access to, personal data.
- "Integrity breach" - where there is an unauthorised or accidental alteration of personal data.
- "Availability breach" - where there is an accidental or unauthorised loss of access to, or destruction of, personal data.

3. Types of 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.

- 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; and
- loss of availability of personal data.

Breaches can be caused by a number of factors:

- Loss or theft of papers/files/data and/ or equipment on which data is stored;
- Inappropriate access to records, allowing unauthorised use;
- Human error;
- Equipment failure;
- Poor data destruction procedures;
- Cyber-attack;
- Hacking.

4. Reporting incidents

All complaints, suspected breaches/incidents should be reported to the School Business Manager (finance@medinahouse.iow.sch.uk) immediately, who will in turn report it to the Corporate Information Unit (cui@iow.gov.uk)

There is a data breach incident reporting form (see Appendix A) to assist staff in reporting incidents. This form should be completed as soon as possible after the breach is reported by the relevant member of staff or their manager. Where information has been sent to, or given to, the wrong recipient, efforts should be made to retrieve the data as soon as possible, where it is safe to do so. The prompt retrieval of information will limit the harm caused and mitigate the risk

The CIU will complete an investigation, on behalf of the Council's Data Protection Officer. The investigation may involve a referral to HR where the actions of a member of staff have caused the breach, and will involve liaising with various colleagues in ICT, legal etc for suitable advice.

In considering the seriousness of the incident, consideration will be taken of:

- The type of breach;
- The nature, sensitivity and volume of personal data;
- Ease of identification of individuals;
- Severity of consequences for individuals;
- Special characteristics of the individuals;
- The number of affected individuals.

5. Determining the level of a breach

To assist in assessing the level of risk involved in a breach, the school/council will continue to use the scoring matrix recommended by the IG Toolkit Incident Reporting Tool (see Appendix B). Where incidents result in a Level 1 or above breach, a self-referral will be made to the ICO unless it is determined that it is unlikely to result in a risk to the rights and freedoms of an individual (as stipulated by the GDPR).

6. Self reporting to the Information Commissioners Office (ICO)

The General Data Protection Regulation (the GDPR) introduces the requirement for a personal data breach to be notified to the competent national supervisory authority, which in the UK is the Information Commissioners Office (ICO) and, in certain cases, to communicate the breach to the individuals whose personal data have been affected by the breach.

The school/ council must report all data breaches to the ICO without undue delay and, where feasible, not later than 72 hours after having become aware of it unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where it is not possible to report within the 72 hours, we must provide reasons for the delay.

Certain information must be provided when reporting a data breach to the ICO, this includes:

(a) nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) describe the likely consequences of the personal data breach;

(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects."

It is recognised that, depending on the nature of a breach, further investigation may be necessary to establish all of the relevant facts relating to the incident. Information may be provided in phases where further details are identified following investigation, but every effort should be made to report as soon as the council becomes aware that a breach may have occurred.

Examples:

- A parent informs the school that they have accidentally received a letter addressed to another parent that includes personal data. The date the parent informed the school is the date that we were made aware.
- The school detects that there has been a possible intrusion into its network. The systems are checked to establish whether personal data held on that system has been compromised and confirms this is the case – this is the date that the school is aware of the breach.

After first being informed of a potential breach or when it has itself detected a security incident, the school may undertake a short period of investigation in order to establish whether or not a breach has in fact occurred. During this period of investigation the school may not be regarded as being "aware". However, it is expected that the initial investigation should begin as soon as possible and establish with a reasonable degree of certainty whether a breach has taken place; a more detailed investigation can then follow.

7. Informing individuals

The school is required to inform data subjects of a data breach, "When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons". The communication of a breach to individuals should be made "without undue delay," i.e. as soon as possible. The main objective of notification to individuals is to provide specific information about steps they should take to protect themselves.

There are 3 situations where controllers are not required to notify individuals of a breach:

- The controller has applied appropriate technical and organisational measures to protect personal data prior to the breach, in particular those measures that render personal data unintelligible to any person who is not authorised to access it. This could, for example, include protecting personal data with state-of-the-art encryption, or by tokenization.
- Immediately following a breach, the controller has taken steps to ensure that the high risk posed to individuals' rights and freedoms is no longer likely to materialise. For example, depending on the circumstances of the case, the controller may have immediately identified and taken action against the individual who has accessed personal data before they were able to do anything with it. Due regard still needs to be given to the possible consequences of any breach of confidentiality, again, depending on the nature of the data concerned.
- It would involve disproportionate effort to contact individuals, perhaps where their contact details have been lost as a result of the breach or are not known in the first place. For example, the warehouse of a statistical office has flooded and the documents containing personal data were stored only in paper form. Instead, the controller must make a public communication or take a similar measure, whereby the individuals are informed in an equally effective manner. In the case of disproportionate effort, technical arrangements could also be envisaged to make information about the breach available on demand, which could prove useful to those individuals who may be affected by a breach, but the controller cannot otherwise contact.

8. Data processors

Where a third party is processing personal data on behalf of the school, they will be considered a data processor. Whilst the school, as data controller, retains overall responsibility for the protection of personal data, the third party (data processor) is required to assist the school in ensuring compliance with the obligations of the data protection legislation. In particular, if the processor becomes aware of a breach of the personal data it is processing on behalf of the controller, it must notify the controller "without undue delay". It should be noted that the processor does not need to first assess the likelihood of risk arising from a breach before notifying the controller; it is the controller that must make this assessment on becoming aware of the breach. The processor just needs to establish whether a breach has occurred and then notify the controller.

9. Documenting breaches

Regardless of whether or not a breach needs to be notified to the ICO, the school must keep details of all breaches (See Appendix D), including the facts relating to the breach, its effects and any remedial action taken. The Corporate Information Unit will maintain a log of all breaches.

Advice and guidance on all matters relating to data protection legislation and confidentiality can be obtained by contacting the Corporate Information Unit, ciu@iow.gov.uk.

APPENDIX A – Data Breach Report Form

This form is for the School Business Manager or Senior Staff to complete, following the initial report of an information incident. It should not take more than 15 minutes to complete.

Please provide as much information as possible. If you do not know the answer or you are waiting on the completion of further enquiries please state this and indicate when this information may be available. In addition to completing the form below, please provide any other supporting information that maybe relevant.

In the wake of an information incident, swift containment and recovery of the situation is vital. Where information has been sent to the wrong recipient immediate efforts should be made to retrieve the information. Every effort should be taken to minimise the potential impact on affected individuals and the Council, and details of the steps taken to achieve this should be included in this form.

Contact Details

Please provide your contact details should we require further information concerning the incident (Name and job title, email address and contact telephone number)	

Details of the information incident

Please describe the incident in as much detail as possible.	
When did the incident happen? (time and date)	
How did the incident happen?	
If there has been a delay in reporting the incident please explain your reason(s) for this.	
What measures and operational controls were in place to prevent and/or detect an incident of this nature occurring?	
Please provide the name and job title of the individual who was responsible for the breach.	

Personal data placed at risk

What, if any, personal data has been placed at risk? Please specify if any financial or personal sensitive data has been affected and provide details of the extent.	
How many individuals does the data relate to?	
Have the affected individuals been made aware that an incident has occurred?	
What are the potential risks, consequences and adverse effects on those individuals?	
Have any of the affected individuals complained about the incident and if so, what action has been taken?	

Containment and Recovery

Has any action been taken to minimise/mitigate the effect on the affected individual(s)? If so, please provide details.	
Has the information placed at risk now been recovered? If so, please provide details of how and when this occurred.	
Have any steps been taken to prevent a recurrence of this incident? If so, please provide details.	
Who have you informed about the incident, both internal and external? For example, in the event of theft, have the Police been informed and do you have a crime number?	

Training and guidance

Please confirm that all employees involved with the incident have successfully completed the Council's mandatory GDPR training?	
Has any additional Information Governance training been provided? If so, please provide details.	
Has any specific detailed operational guidance been developed and provided to staff on handling information, including the use of Council IT equipment? If so, please provide details.	

Previous information incidents

Have you (your department/team) reported any previous information incidents in the last year?	
If the answer is yes, please provide brief details.	

Investigation

Have you asked any questions to determine the circumstances leading to the loss of information? If so, please provide details.	
What, if any actions have been taken to preserve evidence and/or create an audit trail relating to the information incident?	
What, if any, remedial actions have been taken since the information incident occurred to prevent any recurrence?	

Where remedial actions have been identified what timescales have been agreed for their implementation? Please provide details.	

Sending this form

Send your completed form and any related attachments within one day of the date of the incident to ciu@iow.gov.uk with 'Information Incident Report Form' in the subject field.

What happens next?

When we receive this form, we will contact you to provide:

- An incident reference number; and
- Information about our next steps

If you need any help in completing this form, please contact the Corporate Information Unit, ciu@iow.gov.uk or telephone extensions 6329, 6387, 6330 or 6328.

Corporate Information Unit Use Only:	
Reference Number	
Severity / Impact Rating	

APPENDIX B - The following process should be followed to categorise a DPI

Step 1: Establish the scale of the incident. If this is not known it will be necessary to estimate the maximum potential scale point.

Baseline Scale Point	
0	Information about less than 10 individuals
1	Information about 11-50 individuals
2	Information about 51-100 individuals
3	Information about 101-300 individuals
4	Information about 301 – 500 individuals
5	Information about 501 – 1,000 individuals
6	Information about 1,001 – 5,000 individuals
7	Information about 5,001 – 10,000 individuals
8	Information about 10,001 +

Step 2: Sensitivity Factors modify baseline scale point

Low:	**For each of the following factors reduce the baseline score by 1 scale point**
-1 for each	No sensitive personal data or other sensitive information at risk
	Limited demographic data at risk e.g. address not included, name not included
	Security controls/difficulty to access data partially mitigates risk
	Confirmed that there is no link between the data subject and recipient
	Sent to wrong recipient but not received or returned unopened

Medium:	**The following factors have no effect on baseline score**
0	Basic demographic data at risk e.g. equivalent to telephone directory
	Limited sensitive personal data at risk
	Unconfirmed or possible link between data subject and recipient

High:	**For each of the following factors increase the baseline score by 1 scale point**
+1 for each	Detailed or multiple persons sensitive personal information at risk
	Particularly sensitive information at risk
	One or more previous incidents of a similar type in past 12 months
	Failure to securely encrypt mobile technology or other obvious security failing
	Newsworthy aspects or media interest
	A complaint has been made to the Information Commissioner
	Individuals affected are likely to suffer significant distress or embarrassment
	Individuals affected have been placed at risk of physical harm
	Individuals affected may suffer significant detriment e.g. financial loss
	Incident has incurred or risked incurring a clinical untoward incident
	Confirmed link between data subject and recipient

Final Score	**Level of DPI**
0	Level 0 DPI
1 or 2	Level 1 DPI
3 - 5	Level 2 DPI
6 - 8	Level 3 DPI

APPENDIX C - Examples of personal data breaches and who to notify

Example	Notify the ICO?	Notify the data subject?	Notes/ recommendations
(i) A controller stored a backup of an archive of personal data encrypted on a USB key. The key is stolen during a break-in.	No	No	As long as the data are encrypted with a state of the art algorithm, backups of the data exist the unique key is not compromised, and the data can be restored in good time, this may not be a reportable breach. However if it is later compromised, notification is required.
(ii) A brief power outage lasting several minutes at a controller's call centre meaning customers are unable to call the controller and access their records.	No	No	This is not a notifiable breach, but still a recordable incident under Article 33(5). Appropriate records should be maintained by the controller.
(iii) An individual phones a bank's call centre to report a data breach. The individual has received a monthly statement for someone else. The controller undertakes a short investigation (i.e. completed within 24 hours) and establishes with a reasonable confidence that a personal data breach has occurred and	Yes	Only the individuals affected are notified if there is high risk and it is clear that others were not affected.	If, after further investigation, it is identified that more individuals are affected, an update to the supervisory authority must be made and the controller takes the additional step of notifying other individuals if there is high risk to them.

whether it has a systemic flaw that may mean other individuals are or might be affected.			
(iv) Medical records in a hospital are unavailable for the period of 30 hours due to a cyber-attack.	Yes, the hospital is obliged to notify as high-risk to patient's well-being and privacy may occur.	Yes, report to the affected individuals.	
(v) Personal data of a large number of students are mistakenly sent to the wrong mailing list with 1000+ recipients.	Yes, report to supervisory authority.	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	
(vi) A direct marketing e-mail is sent to recipients in the "to:" or "cc:" fields, thereby enabling each recipient to see the email address of other recipients.	Yes, notifying the supervisory authority may be obligatory if a large number of individuals are affected, if sensitive data are revealed (e.g. a mailing list of a psychotherapist) or if other factors present high risks (e.g. the mail contains the initial passwords).	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	Notification may not be necessary if no sensitive data is revealed and if only a minor number of email addresses are revealed.

APPENDIX D

Timeline of Incident Management

Date	Time	Activity	Decision	Name/position	Date