Mill Hill

Instilling values, inspiring minds
Grimsdell | Belmont | Mill Hill School | Mill Hill International

Data Breach Policy 2018/19

Key points of the Data Breach Policy

Purpose	To explain the procedure whenever a data breach occurs.
What to do on becoming aware of a data breach	If a member of Staff becomes aware that a data breach may have or has occurred they MUST take the following steps **immediately**: • Notify the Compliance Manager, Maxine Zeltser, or Operations Manager, Michael Butcher, by email on **compliance@millhill.org.uk** and their line manager. The email should set out the nature of the incident, the date it occurred, those involved and the type of data potentially accessible/accessed/disclosed. • If the breach occurs or is discovered outside of normal working hours, an email should be sent to the compliance manager or operations manager at the above address and their line manager as soon after discovery as possible.

Definitions

The Foundation:
means the Mill Hill School Foundation which comprises the Senior School known as Mill Hill School, The Mount Mill Hill International, Belmont School (the preparatory school) and Grimsdell School (the pre-preparatory school). It is a registered charity and a company limited by guarantee, employing both teaching and non-teaching staff. Legal responsibility rests with the company acting by the Court of Governors, and the Headteachers having day to day responsibility for the management of the schools and the care of pupils

Data Protection Law:
This refers to all relevant legislation including the Data Protection Act 1998 and related statutory instruments (until 25 May 2018); The General Data Protection Regulation (EU 2016/679) from 25 May 2018 and The Data Protection Act 2018 and related legislation from 25 May 2018.

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. Personal data breaches can include:

> 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

Staff:
This refers to all Foundation staff, Governors, volunteers and contractors.

1. Policy Statement
The Foundation holds large amounts of personal and sensitive data. Every care is taken to protect personal data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This procedure applies to all personal and sensitive data held by The Foundation and all Staff. This policy must be read in conjunction with the Foundation's Data Protection Policy, Information Security Policy; Risk Management Policy and Retention of Records Policy.

2. Purpose
This Policy sets out the course of action to be followed by all Staff at The Foundation if a Data Breach occurs.

Recital 85 of the General Data Protection Regulations explains that:

'A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.'

3. Managing a Data Breach

3.1. If a member of Staff becomes aware that a data breach may have or has occurred they MUST take the following steps **immediately**:

> Notify the Compliance Manager, Maxine Zeltser, or Operations Manager, Michael Butcher, by email on **compliance@millhill.org.uk** and their line manager. The email should set out the nature of the incident, the date it occurred, those involved and the type of data potentially accessible/accessed/disclosed.

> If the breach occurs or is discovered outside of normal working hours, an email should be sent to the compliance manager or operations manager at the above address and their line manager as soon after discovery as possible.

3.2. The compliance manager or operations manager must, in liaison with any other relevant member of staff, on receipt of the above notification, immediately establish whether a data breach is still occurring. If so, they should ensure that steps are taken immediately to minimise the effect of the data breach and notify the police and/or the Foundation's insurers, where appropriate.

3.3. The compliance manager or operations manager must, in liaison with any other relevant member of staff, on receipt of any notification of a data breach, whether by a member of Staff as detailed in 3.1 or by a contractor, such as an IT provider, immediately establish the likelihood and severity of the resulting risk to individuals' rights and freedoms. If it is likely that there will be a risk, then either the compliance manager or operations manager should notify the Information Commissioners Office (ICO) without undue delay and, where feasible, **not later than 72 hours of having become aware of the data breach**. A copy of any notification to the ICO should be emailed to the Foundation's Director of Finance and Operations. If the compliance manager or operations manager have notified the ICO of a data breach, a notification of the data breach should also be sent to the Charity Commissioners if necessary.

3.4. If it is considered unlikely that the data breach will result in a risk to the rights and freedoms of individuals then there is no necessity to notify the ICO. The compliance manager or operations manager must keep a record of the basis on which the assessment of the risk was made.

3.5. When reporting a data breach to the ICO, the notification must provide:

> A description of the nature of the data breach including, where possible, the categories and approximate number of individuals concerned and the categories and approximate number of personal data records concerned;

> The name and contact details of the compliance or operations manager or other contact point where more information can be obtained;

> A description of the likely consequences of the personal data breach; and

> A description of the measures taken, or proposed to be taken, to deal with the data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

In the event that it has not been possible to fully investigate the data breach within 72 hours of having become aware of it, the notification should explain that not all the relevant details are yet available and when it is expected that this information will be available. This additional information should be provided by the compliance manager or operations manager to the ICO without delay on it being made available.

A data breach can be reported to the ICO by calling their helpline on 0303 123 1113. The helpline is open Monday to Friday 9am to 5pm but closes at 1pm on Wednesdays. The helpline can offer advice about whether data subjects need to be informed of the data breach. Alternatively, for those cases where the Foundation is confident that that the breach has been dealt with appropriately, the breach can be reported online by sending the notification using the ICO's security breach notification form to casework@ico.org.uk or be reported by post to the ICO office address: Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

3.6. If the compliance manager or operations manager consider that the data breach is likely to result in a high risk to the rights and freedoms of individuals, then those individuals must be notified as soon as possible. The compliance manager or operations manager must keep a record of the basis on which the assessment of the risk was made. This notification should describe, in clear and plain language, the nature of the data breach and, at least:

> A description of the likely consequences of the data breach; and

> A description of the measures taken, or proposed to be taken, to deal with the data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

3.7. The compliance manager or operations manager shall immediately appoint a suitable member of Staff to fully investigate the data breach ('the Investigating Officer'). The Investigating Officer should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation should consider:

> The type of data;

> Its sensitivity;

> What protections were in place (eg. Encryption);

> What has happened to the data;

> Whether the data could be put to any illegal or inappropriate use;

> How many people are affected;

> What type of people have been affected (such as pupils, staff members, suppliers) and whether there are wider consequences to the breach.

A clear record should be made of the nature of the breach and the actions taken to mitigate it. The investigation should be completed urgently and, whenever possible, within 24 hours of the data breach being discovered/reported. The Investigating Officer should take appropriate steps to recover data and minimise risk including:

> Informing people/agencies such as the police, banks, relevant contractors and server administrator;

> Reporting and attempting to recover lost equipment;

> Informing the Foundation's marketing department with a view to managing a press release about the data breach;

> Informing Staff about the data breach and to warn them of possible 'blagging attempts';

> Accessing back-ups to replace lost or damaged data;

> If the data breach included entry codes or passwords, then these must be changed immediately and involved users informed.

4. Ongoing Evaluation, Monitoring and Remediation

Once the data breach has been contained, the Investigating Officer should provide a report to the compliance manager and operations manager setting out both the causes of the data breach and the effectivenesss of the Foundation's response. The review should include the following considerations:

> Where and how personal data is held and where and how it is stored;

> Where the biggest risks lie including identifying any further potential weak points within the existing security measures;

> Whether methods of transmission are secure and the sharing of data limited to the minimum necessary;

> Staff awareness;

> Implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security;

> Whether any changes to systems, policies and procedures should be undertaken.

If systemic or ongoing problems are identified, then an action plan must be drawn up to remedy these. If the data breach warrants a disciplinary investigation, this should be carried out in accordance with the Foundation's Staff Disciplinary Policy. A report should be provided to the compliance manager who will be responsible for monitoring the progress of the action plan. A copy of the report should be forwarded to the Director of Finance and Operations.

5. Staff Training

The Foundation will ensure that that staff are aware of the provisions of its Data Protection Policy and other associated policies and their requirements regarding the handling of personal data including the procedures contained in this Policy. Such training should be part of staff induction and ongoing training and supervision.

6. Data Response Action Plan Summary

Members of staff are referred to the Data Response Action Plan which is annexed to this Policy as Appendix 1 as a summary of their obligations in the event of a data breach.

APPENDIX 1

STEP GUIDE TO DATA BREACH RESPONSE

(to form part of the school's response plan)

1. Upon the first employee becoming aware of the breach

> Am I the relevant person at the organisation? If not, immediately notify that person.

2. Initial assessment, containment and recovery – first few hours:

> How long has the breach been active, what data was involved and how far has it got?

> What immediate steps can be taken to prevent it going further? Consider:

> if a cyber breach, involve the school's IT personnel from the outset;

> if human actor(s) are involved, can they be contacted to give reassurances;

> if e.g. Royal Mail, courier, IT or other contractors are involved, can they assist;

> are specialists needed: forensic IT consultants, crisis management PR, legal etc.

3. Ongoing assessment of risk and mitigation – first 72 hours (and initial notification where required):

> Build up a more detailed picture of the risk and reach of the security breach:

> how many have been affected?

> was any sensitive personal data involved – health, sexual life, crime?

> was financial data involved and/or is there a risk of identify fraud?

> Identify if a crime has been committed and involve police or cyber fraud unit.

> Assess if insurers need notifying (major loss, crime, or possible legal claim(s))

> Decide if the likely risk of harm to the data subjects:

> is sufficient to require a full or preliminary notification to the ICO; and

> If not, is this a matter we can document but deal with internally?; or

> If so, what can we usefully tell the ICO and/or individuals at this stage?

> e.g. provide fraud or password advice, offer counselling etc.

4. Ongoing evaluation, monitoring and remediation:

> Continue to monitor and assess possible consequences (even if apparently contained).

> Keep the ICO and/or those affected informed as new information becomes available.

> Tell the ICO and/or those affected what you are doing to remediate and improve practice.

> Begin process of review internally:

> how did this happen? What could we have done better?

> would training or even disciplinary action be justified for staff members?

> were our policies adequate, and/or adequately followed?

> if our contractors were involved (e.g. systems providers), did they respond adequately? Do we have any remedies against them if not?

5. Record keeping and putting outcomes into practice:

> Keep a full internal record, whether or not the matter was reported or resulted in harm.

> Log this record against wider trends and compare with past incidents.

> Make sure all past outcomes were in fact put into practice.

> Ensure any recommendations made by, or promised to, the ICO are actioned.

> Notify the Charity Commission as an RSI, if a charity, at an appropriate juncture.

> Review policies and ensure regular (or specific, if required) training is actually completed.

Serious breaches should be reported to the ICO using the security breach helpline on 0303 123 1113 (open Monday to Friday, 9am to 5pm). Select option 3 to speak to staff who will record the breach and give advice.

Or, use the security breach notification form, which should be sent to the email address: **casework@ico.org.uk** or by post to the ICO office address: Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

The security breach notification form can be found here:

https://ico.org.uk/media/fororganisations/documents/2666/security_breach_notification_form.doc

Dated: 21 May 2018
To be reviewed: May 2020
Ratified by the Nominations and Governance Committee and signed by its Chair Andrew Welch

Instilling values, inspiring minds
millhill.org.uk

Mill Hill School
The Ridgeway
Mill Hill Village
London NW7 1QS

020 8959 1176
millhill.org.uk