Personal Data Breach and Subject Access Request Policy November 2020

Contents

Plan administration	
Version number	1.0
Date of issue	Nov 2020
Electronic copies of this plan are available from	Staff network drive & Google drive for Govs
Hard copies of this plan are available from	On request from the Business Manager
Date of next review	Nov 2022
Person(s) responsible for review	Mrs Katherine Yates / Mrs Lynne Butterfield
Head's signature	Date:
Chair of Governor's Signature	Date:

1. Introduction

This procedure is based on guidance on personal data breaches [https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/] produced by the Information Commissioners Office.

Data breaches must be reported to the ICO within 72 hours of the breach of personal data.

The General Data Protection Regulation defines personal data as "any information relating to an identified or identifiable natural person ('data subject')"

This policy should be read in conjunction with the Data Protection Policy as that document provides a more detailed look

2. Data Protection Officer

Schools must appoint a Data Protection Officer ["DPO'] and we have elected to use

Craig Stilwell

Company: Judicium Consulting Ltd

Address: 72 Cannon Street, London, EC4N 6AE

Email: dataservices@judicium.com

Telephone: 0203 326 9174

Our in-house DPO, for day to day advice on processes and data protection requirements is Lynne Butterfield. For the purposes of this policy further reference to DPO relates to in-house provision unless stated otherwise.

3. Personal Data Breach

Actions to be taken upon discovery of a personal data breach.

- On finding or causing a breach, or potential breach, the staff member or data processor* must immediately notify the DPO

*A data processor is A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller

- The DPO will investigate the report in liaison with Judicium's DPO, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people

- The DPO will alert the Head teacher and the Chair of Governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)

- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school network location T:\Business Manager\GDPR\Breach\Decisions.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website [https://ico.org.uk/for-organisations/report-a-breach/] within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts and cause
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored T:\Business Manager\GDPR\Breach

- The DPO and Head teacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

4. Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the IT support third party to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Third party / Data Processor breach due to hack

- The DPO will liaise with the Data Processor to ascertain the type and extent of the breach
- The DPO will ensure the ICO is informed of the breach within 72 hours
- All new third party agreements will include a GDPR clause to ensure the Data Processor is aware of data protection responsibilities, including detailed response processes and timescales

Theft of school hardware such as laptops and portable memory drives

- The member of staff responsible for the hardware will alert the DPO in the first instance
- The DPO will determine the data contained on the stolen hardware and list the data types and security systems in place (such as password protected encrypted drives). A decision will then be made with regards to confirmation of a breach
- Where possible the DPO will remotely wipe data from hardware (such as hardware linked to the school GSuite) and record the action
- Where remote deletion is not viable or fails the DPO will presume a data breach and liaise with ICO

Staff Awareness

- Staff will receive regular updates and training on data protection matters through staff meetings, as part of staff weekly memos and face to face training
- GDPR will be discussed during the induction process of new employees and a record kept by the DPO
- All staff will complete and online GDPR Level 2 course and the DPO will record completion
- The DPO will conduct random “information audits” to remind staff about the importance of data protection, provide advice and guidance as necessary, and to determine any risks

5. Subject Access Requests

Individuals have the right to access the personal data and supplementary information school holds about them. This allows them to be aware of, and verify the lawfulness of, school processing this data.

This right applies to everyone whose personal data held by school, including staff, governors, volunteers, parents and pupils.

Requests must be made in writing and the response must be returned within one month. A charge cannot be levied.

6. SAR Process

- Staff must forward to the DPO any request for personal data
- A request may not use the term “Subject Access Request” but if the data requested is personal it is an SAR

On receiving a request the DPO will

- Telephone the individual to confirm a request has been submitted
- Use “reasonable means” to verify the identity of the individual (usually two forms of ID but not necessary if people are known, such as staff or governors)
- If the request is deemed complex the DPO will write to the individual to advise the complexity will require a time extension. This can be up to three months from the original request date
- If the request is made electronically the response should be in a commonly used electronic format

'Unfounded or excessive' requests

, Usually 'unfounded or excessive' means that the request is repetitive, or asks for further copies of the same information. If the request is unfounded or excessive the DPO can

- Charge a reasonable fee for school to comply, based on the administrative cost of providing the information
- Refuse to respond
- Comply within 3 months, rather than the usual deadline of 1 month. The individual must be informed in writing before the first month deadline as to the reason(s) for the delay

Refusing a request

If a request is refused the DPO must

- Respond to the individual within 1 month
- Explain why the requests are refused
- Tell the individual they have the right to complain to the ICO

Appendix 1

A template subject access form is shown overleaf and this may assist people wanting to make a request.

Date: / /

Mount Primary School

Mount Pleasant Road

Wallasey

Merseyside

CH45 5HU

Re: subject access request

Dear Mrs Butterfield,

Please provide me with the information about me that I am entitled to under the General Data Protection Regulation. This is so I can be aware of the information you are processing about me, and verify the lawfulness of the processing.

Here is the necessary information:

Name	
Relationship with the school	Please select: Pupil / parent / employee / governor / volunteer Other (please specify):
Correspondence address	
Contact number	
Email address	
Details of the information requested	Please provide me with: *Insert details of the information you want that will help us to locate the specific information. Please be as precise as possible, for example:* • *Your personnel file* • *Your child's medical records* • *Your child's behavior record, held by [insert class teacher]* • *Emails between 'A' and 'B' between [date]*

If you need any more information from me, please let me know as soon as possible.

Please bear in mind that under the GDPR you cannot charge a free to provide this information, and in most cases, must supply me with the information within 1 month.

If you need any advice on dealing with this request, you can contact the Information Commissioner's Office on 0303 123 1113 or at www.ico.org.uk

Yours sincerely,

Print name: *Sign name:*