

DATA BREACH INCIDENT

MANAGEMENT PROCESS

Prepared: March 2018

Adopted: May 2018

Review: March 2019

# Personal data breach procedure

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 ICO.

* On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
* The DPO will investigate the report, 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 headteacher 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 in GDPR in a locked cupboard and on the School’s Computer system.
* 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.
* 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 in GDPR file in a locked cupboard or on the school’s computer system.

* The DPO and Lead 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

**Actions to minimise the impact of data breaches**

We will take actions set out in the school’s Data Impact Assessment 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.

**Please see the school’s Data Impact Assessment for more information.**

## **Evaluation of Incident Severity**

The severity of the incident will be assessed per the School’s Data Breach Incident Management Process. Assessment would be made based upon the following criteria:

|  |  |
| --- | --- |
| **High Criticality: Major Incident**  | **Contact:**  |
| * Highly Confidential/Confidential Data
* Personal data breach involves > 1000 individuals
* External third-party data involved
* Significant or irreversible consequences
* Likely media coverage
* Immediate response required regardless of whether it is contained or not
* Requires significant response beyond normal operating procedures

  | Lead Responsible Officer * To be determined by the Incident Management Team.

 Other relevant contacts * Lead Teacher
* Representative from school’s Board of Governors
* Internal senior staff as required
* Contact external parties as required i.e. police/ICO/individuals impacted

   |
| **Moderate Criticality: Serious Incident**  | **Contact:**  |
| * Confidential Data
* Not contained within School
* Breach involves personal data of more than 100 individuals
* Significant inconvenience will be experienced by individuals impacted
* Incident may not yet be contained
* Incident does not require immediate response
* Incident response may require notification to School’s senior managers

  | Lead Responsible officer * Lead Teacher/DPO

Other relevant contacts: * Representative from school’s Board of Governors
* Internal senior staff as required
 |
| **Low Criticality: Minor Incident**  | **Contact:**  |
| * Internal or Confidential Data
* Small number of individuals involved
* Risk to School low
* Inconvenience may be suffered by individuals impacted
* Loss of data is contained/encrypted
* Incident can be responded to during working hours Example:
* Email sent to wrong recipient
* Loss of encrypted mobile device
 | Lead Responsible Officer * Lead Teacher / DPO (May delegate responsibility to another appropriate senior member of staff)

 Other relevant contacts: * Governance Team to follow up on policy procedures for managing personal data breaches
 |

## **Data Breach Checklists**

1. Containment and Recovery
2. Assessment of Risks
3. Consideration of Further Notification
4. Evaluation and Response

|  |  |  |
| --- | --- | --- |
| **Step**  | **Action**  | **Notes**  |
| **A**  | **Containment and Recovery:**  | **To contain any breach, to limit further damage as far as possible and to seek to recover any lost data.**  |
| 1  | Lead Teacher or DPO to ascertain the severity of the breach and determine if any personal data is involved.  | See Appendix 1 of Data Breach Policy |
| 2  | Lead Teacher or DPO to involve Chair of Board and Gov. responsible for investigating breach and forward a copy of the data breach report (if required) | To oversee full investigation and produce report. Ensure lead has appropriate resources including sufficient time and authority. If personal data has been breached also contact DPO. In the event that the breach is severe the Board will lead the initial response.  |
| 3  | Identify the cause of the breach and whether the breach has been contained?  Ensure that any possibility of further data loss is removed or mitigated as far as possible  | Establish what steps can or need to be taken to contain the breach from further data loss. Contact all relevant departments who may be able to assist in this process.  This may involve actions such as taking systems offline or restricting access to systems to a very small number of staff until more is known about the incident.   |
| 4 | Determine whether anything can be done to recover any losses and limit any damage that may be caused  | E.g. physical recovery of data/equipment, or where data corrupted, through use of back-ups.  |
| 5  | Where appropriate, the Lead Responsible Officer or nominee to inform the police.  | E.g. stolen property, fraudulent activity, offence under Computer Misuse Act.   |
| 6  | Ensure all key actions and decisions are logged and recorded on the timeline.   |   |

|  |  |  |
| --- | --- | --- |
| **B**  | **Assessment of Risks**  | **To identify and assess the ongoing risks that may be associated with the breach.**  |
| 7 | What type and volume of data is involved?  |  Data Classification/volume of individual data etc  |
| 8 | How sensitive is the data?  | Sensitive personal data? By virtue of definition within Data Protection Act (e.g. health record) or sensitive because of what might happen if misused (banking details).  |
| 9  | What has happened to the data?  | E.g. if data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged, this poses a different type and level of risk.  |
| 10 | If the data was lost/stolen, were there any protections in place to prevent access/misuse?  | E.g. encryption of data/device.  |
| 11  | If the data was damaged/corrupted /lost, were there protections in place to mitigate the impact of the loss?  | E.g. back-up tapes/copies.  |
| 12  | How many individuals’ personal data are affected by breach?  |  |
| 13  | Who are the individuals whose data has been compromised?  | Students, applicants, staff, customers, clients or suppliers?  |
| 14  | What could the data tell a third party about the individual? Could it be misused?  | Consider this regardless of what has happened to the data. Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people.  |
| 15  | Is there actual/potential harm that could come to any individuals?  | E.g. are there risks to: * physical safety;
* emotional wellbeing;
* reputation;
* finances;
* identify (theft/fraud from release of non-public identifiers);
* or a combination of these and other private aspects of their life?
 |
| 16  | Are there wider consequences to consider?  | E.g. a risk to public health or loss of public confidence in an important service we provide?  |
| 17  | Are there others who might advise on risks/courses of action?  | E.g. If individuals’ bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use.  |

|  |  |  |
| --- | --- | --- |
| **C**  | **Consideration of Further Notification**  | **Notification is to enable individuals who may have been affected to take steps to protect themselves or allow the regulatory bodies to perform their functions.**  |
| 18 | Are there any legal, contractual or regulatory requirements to notify?  | E.g.: terms of funding; contractual obligations  |
| 19  | Can notification help the School meet its security obligations under the seventh data protection principle?  | E.g. prevent any unauthorised access, use or damage to the information or loss of it.  |
| 20  | Can notification help the individual?  | Could individuals act on the information provided to mitigate risks (e.g. by changing a password or monitoring their account)?  |
| 21 | If a large number of people are affected, or there are very serious consequences, inform the Information Commissioner’s Office (through the Director of Information).  | DPO to work with School Incident Management Team |
| 22  | Consider the dangers of ‘over notifying’.  | Not every incident will warrant notification “and notifying a whole 2 million strong customer base of an issue affecting only 2,000 customers may well cause disproportionate enquiries and work”.  |
| 23  | Consider whom to notify, what you will tell them and how you will communicate the message.  | * There are a number of different ways to notify those affected so consider using the most appropriate one. Always bear in mind the security of the medium as well as the urgency of the situation.
* Include a description of how and when the breach occurred and what data was involved. Include details of what has already been done to respond to the risks posed by the breach.
* When notifying individuals give specific and clear advice on the steps they can take to protect themselves and also what the institution is willing to do to help them.
* Provide a way in which they can contact us for further information or to ask questions about what has occurred (e.g. a contact name, helpline number or a web page).
 |
| 24  | Consult the ICO guidance on when and how to notify it about breaches.      | Where there is little risk that individuals would suffer significant detriment, there is no need to report. There should be a presumption to report to the ICO where a large volume of personal data is concerned and there is a real risk of individuals suffering some harm. Cases must be considered on their own merits and there is no precise rule as to what constitutes a large volume of personal data. Guidance available from [http://www.ico.gov.uk/ for\_organisations/data\_protection/ the\_guide/principle\_7.aspx](http://www.ico.gov.uk/%20for_organisations/data_protection/%20the_guide/principle_7.aspx)  |
| 25  | Consider, as necessary, the need to notify any third parties who can assist in helping or mitigating the impact on individuals.  | E.g. police, insurers, professional bodies, funders, trade unions, website/system owners, bank/credit card companies.  |

|  |  |  |
| --- | --- | --- |
| **D**  | **Evaluation and Response**  | **To evaluate the effectiveness of the School’s response to the breach.**  |
| 26  | Establish where any present or future risks lie.  |   |
| 27 | Consider the data and contexts involved.  | E.g. what data is held, its extent, sensitivity, where and how it is stored, how long it is kept.  |
| 28  | Consider and identify any weak points in existing security measures and procedures.  | E.g. in relation to methods of storage and/or transmission, use of storage devices, levels of access, systems/network protections.  |
| 29  | Consider and identify any weak points in levels of security awareness/training.  | Fill any gaps through training or tailored advice.  |
| 30 | Report on findings and implement recommendations.  | DPO to report to Lead Teacher and Board of Governors |

**Appendix 1: Timeline of Incident Management**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date**  | **Time**  | **Activity**  | **Decision**  | **Authority**  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |