

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

Data Breach Policy

Prepared: April 2018 v0.1

Adopted: May 2018

Reviewed: April 2019

**Contents**

[1. Background 2](#_Toc26153)

[2. Aim 2](#_Toc26154)

[3. Definition 3](#_Toc26155)

[4. Scope 3](#_Toc26156)

[5. Responsibilities 3](#_Toc26157)

[6. Data Classification 3](#_Toc26158)

[7. Data Security Breach Reporting 4](#_Toc26159)

[8. Data Breach Management Plan 4](#_Toc26160)

[9. Authority 5](#_Toc26161)

[10. Review 5](#_Toc26162)

[11. References: 5](#_Toc26163)

 **Document Information & Version History:**

* v0.1 – April 2018

# Background

Data 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.

# Aim

The aim of this policy is to standardise the School-wide response to any reported data breach incident and ensure that they are appropriately logged and managed in accordance with best practice guidelines.

By adopting a standardised approach to all reported incidents, it aims to ensure that:

* incidents are reported in a timely manner and can be properly investigated
* incidents are handled by appropriately authorised and skilled personnel
* appropriate levels of School management are involved in response management
* incidents are recorded and documented
* the impact of the incidents is 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
* 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 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
* Equipment failure
* Human error
* Unforeseen circumstances such as a fire or flood
* Hacking attack
* ‘Blagging’ offences where information is obtained by deceit

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

# Scope

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

# Responsibilities

5.1 Information users

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.

5.2 Lead Teacher of School

Lead Teacher is responsible for ensuring that staff act in compliance with this policy and assist with investigations as required.

5.3 Data Protection Officer

Data Protection Officer will be responsible for overseeing management of the breach in accordance with the Data Breach Management Plan. Suitable delegation may be appropriate in some circumstances.

5.4 Contact Details

In the event that the Incident Management Team need to be contacted, the school should be contacted on 020 8575 0237.

# 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.

All reported incidents will need to include the appropriate data classification for assessment of risk to be conducted. Data classification referred to in this policy means the following Data Categories:

6.1 Public Data:

Information intended for public use, or information which can be made public without any negative impact for the School.

6.2 Internal Data:

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

6.3 Confidential Data:

Information of a more sensitive nature for the business and academic operations of the School, representing the basic intellectual capital and knowledge. Access should be limited to only those people that need to know as part of their role within the School.

6.4 Highly confidential Data:

Information that, if released, will cause significant damage to the School's business activities or reputation, or would lead to breach of the Data Protection Act. Access to this information should be highly restricted.

# Data Security Breach Reporting

Confirmed or suspected data security breaches should be reported promptly to the Lead Teacher on 020 8575 0237, email: sionedjones@ysgolgymraegllundain.co.uk) or the school’s Data Protection Officer, email jonathanwright@ysgolgymraegllundain.co.uk The report should include full and accurate details of the incident including who is reporting the incident and what classification of data is involved. Where possible the incident report form should be completed as part of the reporting process. See **Appendix 1.**

Once a data breach has been reported an initial assessment will be made to establish the severity of the breach and who the lead responsible officer to lead should be.

All data security breaches will be centrally logged in the school’s GDPR file to ensure appropriate oversight in the types and frequency of confirmed incidents for management and reporting purposes.

# Data Breach Management Plan

The management response to any reported data security breach will involve the following four elements.

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

Each of these four elements will need to be conducted in accordance with the school’s Data Breach Incident Management Process.

# Authority

Staff, pupils, contractors, consultants, visitors and guests who act in breach of this policy, or who do not act to implement it, may be subject to disciplinary procedures or other appropriate sanctions.

# Review

The Lead Teacher and DPO will monitor the effectiveness of this policy and carry out regular reviews of all reported breaches.

# References:

Information Commissioner:

<https://ico.org.uk/media/1562/guidance_on_data_security_breach_management.pdf>

## Appendix 1: Incident Report Form

|  |  |
| --- | --- |
| **Description of the Data Breach:**  |   |
| **Time and Date breach was identified and by whom.**  |   |
| **Who is reporting the breach: Name/Post/Dept**  |   |
| **Contact details:** **Telephone/Email**  |   |
| **Classification of data breached** (in accordance with University Security Policy) i.Public Data ii. Internal Data iii. Confidential Data iv. Highly confidential Data |   |
| **Volume of data involved**  |   |
| **Confirmed or suspected breach?**  |   |
| **Is the breach contained or ongoing?**  |   |
| **If ongoing what actions are being taken to recover the data**  |   |
| **Who has been informed of the breach**  |   |
| **Any other relevant information**  |   |

Email form to Lead Teacher / DPO: sionedjones@ysgolgymraegllundain.co.uk / jonathanwright@ysgolgymraegllundain.co.uk

Call 020 8575 0237 and advise that a Data Security Breach report form is being sent.

|  |  |
| --- | --- |
| Received by:  |   |
| Date/Time:  |   |

##