St Bartholomew's School
Data Breach Policy
May 2018

1. Introduction

St Bartholomew's School is committed to compliance with applicable UK and EU laws in respect of personal data and in accordance with the General Data Protection Regulation (GDPR).

This commitment extends to adhering to a robust and systematic process to identifying, managing and reporting personal data breaches, to ensure the organisation can act responsibly and protect its personal information as far as possible.

2. Scope of the Policy

This Policy covers:

a) Suspected and confirmed data breaches - '*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.'*

   Other definitions within this Policy are as per the Data Protection Policy.

b) all personal information processed in any format.

c) personal information relating to all individuals (including students, staff, governors, visitors, contractors and data processors acting on behalf of St Bartholomew's School).

The Policy does not cover other security incidents (such as impersonation, denial of service and website defacement) that do not involve the loss or theft of personal data - organisations are not required to report these security incidents, but they are required by law to follow procedures in the case of data breaches.

3. Purpose of the Policy

The purpose of this Policy is to document and standardise St Bartholomew's School response to any personal data breach.

This means that suspected breaches are recognised and then escalated by employees or other parties; that the suspected breach is immediately investigated, controlled and responded to; that external bodies or any data subjects impacted are informed, as required; breaches are recorded; and, that the breach is reviewed to identify improvements in policies and procedures.

4. Responsibilities

The Data Protection Officer (DPO) has overall responsibility for School adherence to this policy.

The Data Breach Investigation Team (set up by DPO) is responsible for dealing with suspected breaches.

Every employee has a personal responsibility for the implementation of this Policy and for identifying and escalating a suspected breach. Failure to comply with this Policy may lead to disciplinary action; in serious cases, such behaviour may reasonably be deemed to constitute gross misconduct.

Other parties (for example, data processors) have a responsibility for the implementation of this Policy (alongside other relevant policies) and for identifying and escalating a suspected breach about personal information controlled by St Bartholomew's School and processed by the party. Other parties who act in breach of this Policy, or who do not act to implement it, may be subject to other appropriate sanctions.

5. Breach Management

5.1 Identifying a Significant Data Breach

Employees and other parties are encouraged to think broadly about that constitutes a personal data breach and to err on the side of caution – if it may be a breach, treat it as a breach.

Some data breaches are less critical and are best dealt with by improving our procedures and training, for example, leaving your computer on when you pop away from your desk, or inadvertently leaving a letter on the printer. In these cases, please feedback to the DPO so that all staff can be reminded of their day to day obligations.

However, more significant personal data breaches need to be escalated to the DPO as they may need to be reported.
For example:

- Loss or theft of data or equipment on which data is stored e.g. loss of a laptop or a paper file containing student or staff health records;
- Unauthorised access to confidential or highly confidential data e.g. a non-employee viewing sensitive information access to which they are not entitled;
- Human error leading to the loss of data e.g. sending an email containing sensitive data to the wrong recipient;
- Unforeseen circumstances such as a fire or flood, power outage;
- Hacking, phishing and other 'blagging' attacks where information is obtained by deceiving whoever holds it.

5.2 Escalating a Data Breach

Any significant breach that is likely to result in harm to data subjects must be reported by the School to the Information Commissioner without undue delay, and in any event within 72 hours.

So, if an employee or other party knows or suspects that a significant data breach has occurred or may occur, they should immediately, and as a priority, make contact with the DPO by emailing DPO@stbarts.co.uk , phoning 01635 521255 and/or coming in person.

The employee or other party may be asked by the DPO to complete a Data Breach Report Form (Appendix 1), as St Bartholomew's School is required to maintain records of all significant data breaches comprising the facts and effects of the breach and any remedial action taken.

If staff or other parties know or suspect that a Personal Data Breach has occurred, they must not attempt to investigate the matter but must immediately contact the DPO. All evidence must be preserved relating to the potential Personal Data Breach.

5.3 Reviewing the Data Breach

On being notified of a suspected data breach, the DPO will review the suspected breach and either:

a) determine that it is not a breach, or is insignificant in nature; then put in place any procedure to remove any future risk; or
b) assemble a Data Breach Investigation Team of appropriate stakeholders, who will review the details of the suspected breach and determine the appropriate plan of action.

5.4 Breach Management

If a significant breach has occurred, the Data Breach Investigation Team will work with appropriate advisers as required and follow these four summary steps:

1. Containment and recovery;
2. Assess and record the breach;
3. Notify appropriate parties, if appropriate (this may include the affected data subjects; a public notice of the breach, and reporting to relevant regulators);
4. A plan to prevent future breaches.

5.5 Data Breach Reporting of significant breaches

St Bartholomew's School is required to maintain records of all significant data breaches comprising the facts and effects of the breach and any remedial action taken. The reporting of breaches is the responsibility of the DPO who will inform the HeadTeacher in the event of a breach arising, and will report to them its full details and status.

6. Authority

Failure to comply with this Policy and associated policies (*e.g.* Data Protection or Information Security) puts personal data at risk.

Failure to notify the DPO of an actual or suspected significant data security breach is a very serious issue. Employees may be liable to disciplinary action if they fail to comply with the provisions of this, and all related plans, policies and procedures.

Other parties who act in breach of this Policy, or who do not act to implement it, may be subject to other appropriate sanctions.

7. Policy Management

Publication - This policy shall be available through the DPO and the school website: stbarts.co.uk

Revisions - The DPO is responsible for the maintenance and accuracy of this policy. This Policy will be reviewed on an annual basis.

Other Documents and Policies
This policy supplements St Bartholomew's School other policies relating to personal information, including but not limited to:

- Data Protection Policy
- Information Security Policy
- Records and Data Retention Policy
- Rights and Requests (DSAR) Policy
- Staff Acceptable Use Policy (IT Systems and Data)
- Staff Handbook
- Staff Privacy Notice
- Student Privacy Notice
- Parents Handbook

APPENDIX 1

ST BARTHOLOMEW'S SCHOOL
SIGNIFICANT DATA BREACH REPORT FORM

If you know or suspect a data security breach has occurred, immediately and as a priority contact the DPO: DPO@stbarts.co.uk, tel: 01635 521255 or in person.

You may then be asked to complete this Data Breach report form and return it to the DPO.

Name and contact details of person notifying the actual or suspected breach	*Insert your name , and contact details*
Faculty/Manager/Other Party	*Insert department from which the report emanated and the relevant manager or details of other party*
Date of actual or suspected breach	*Insert date*
Date of discovery of actual or suspected breach	*Insert date*
Date of this report	*Insert date*
Summary of the facts	*Provide as much information as possible—including the amount, sensitivity and type of data involved and any systems or devices involved – please use a separate sheet if necessary*
Cause of the actual or suspected breach (if known)	P*rovide a detailed account of what happened*
Is the actual or suspected breach ongoing?	*Yes or No*
Who is or could be affected by the actual or suspected breach?	*Include details of categories and approximate number of individuals affected.*

	Do not notify affected data subjects. The data breach team will determine who should be notified and how.
Are you aware of any related or other data breaches?	Yes or No *If yes, provide more details*

Email or deliver this form to the DPO at DPO@stbarts.co.uk
or, present it in person to DPO, St Bartholomew's School, Andover Road, Newbury, Berkshire, RG14 6JP