PLYMOUTH HIGH SCHOOL FOR GIRLS

POLICY: DATA BREACH MANAGEMENT PROCEDURE and DATA BREACH DEFINITION POLICY

SLT LINK MEMBER:	**Shaun Willis**
GOVERNORS SUB COMMITTEE:	**P & R**
This policy was adopted/updated:	May 2018
This policy will be reviewed:	September 2020
Statutory Policy:	NO
Source:	LA/School

Contents

DATA BREACH MANAGEMENT PROCEDURE

Plymouth High School holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the event of 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 Plymouth High School and all school staff, Governors, volunteers and contractors, referred to herein after as 'staff'.

This policy sets out the course of action to be followed by all staff at the Plymouth High School if a data protection breach takes place.

1.0 IDENTIFYING A BREACH

1.1 Identification

If any member of staff finds or has reported to them an actual breach or 'near miss' breach of personal data they must complete the 'Data Breach Report - Initial Details' (see Appendix 1).

Please refer to the Data Breach Management Policy for the definition of what is considered a breach to see if this procedure needs to be followed.

1.2 How were we notified?

In order to take appropriate actions we need to establish how we were notified e.g.:

Staff member	Partner	Parent/carer or pupil
Member of the Public: • Escalate to DPO • Do we need to put a communication together for the press? • Are they taking further action?	News article: • Escalate to DPO / Headteacher / Governors • Prepare a communications statement for the press	Other: • Please contact DPO for advice

1.3 Initial Actions

In order to minimise the loss of personal data and to protect personal data from further loss immediate action must be taken.

The staff member must complete the 'Initial actions' outlined at the start of the 'Data Breach Report – Initial Details' form (Appendix 1). These are:

1. If possible, recover the data / document as soon as possible
2. Stop further data loss (see Part 2.0 Containment below)
3. Consult with a manager / headteacher
4. Report the incident

* The report must be emailed to dataprotectionofficer@plymouth.gov.uk for the Data Protection Officer's (DPO) attention at the latest by close of business on the day of identification, if the breach was identified before 1pm, or by 12pm the following day for breaches identified after 1pm. Breaches that need to be reported to the Information

Commissioner must be notified to them within 72 hours therefore the 'Initial Details' form should be sent to the DPO sooner than the times specified if possible.

** In the case of electronic breaches the schools IT Manager must also be notified.

2.0 CONTAINMENT

Upon receipt of the notification, the DPO will take all reasonable steps, not already undertaken, to contain and minimise the impact of the breach. We will review the effectiveness of these actions and amend them as necessary after any data breach.

- Is the breach paper or electronic?
  - ❖ Paper
    - Recover the document
    - Identify how the breach occurred
    - ➢ Post
      - Do we need to stop any further post going out?
    - ➢ By Hand
      - Is this an isolated incident?
    - ➢ Other
      - Please contact Data Protection Officer for advice
        - Identify whether anyone else may have been affected
    - ➢ Recover the documents
  - ❖ Electronic
    - ➢ Email
      - Can the email be recalled?
        - Emails can only be recalled if the recipients are internal
      - Can the recipient delete the email?
        - Both from inbox and deleted items
      - Ask the recipient to confirm they have complied with the request to delete?
    - ➢ Removable media
      - Was the media encrypted?
      - Has the data been copied?
      - Has the data been passed onto a 3rd party?
      - Can the media be recovered?
    - ➢ Portable devices (laptops/tablets)
      - Was the device encrypted?
      - Was the device password protected?
      - Has the data been copied?
      - Has the data been passed onto a 3rd party?
      - Can the device be recovered?
    - ➢ Other
      - Please contact Data Protection Officer for advice

The DPO will carry out an internet search to check that the information has not been made public; if it has been request that the information is removed from the website and deleted.

3.0 ASSESSMENT

The DPO will:

- Identify the type of data
- Identify the sensitivity of data
- Identify number of people affected
- Provide a description of the likely consequences of the personal data breach
- Identify any measures needed to help those affected
- Identify the cause of breach
- Analyse the breach to determine what the impact will be. This will be an assessment of the impact on the data subject of the particular aspect of the breach.
- Complete the Data Breach Investigation Report (see Appendix 2).

* Staff will cooperate fully during the assessment process.

4.0 NOTIFICATION

The DPO, in agreement with the schools Headteacher / Board of Governors / Trust will:

- Create a communication plan to include:
    - ❖ Details of who needs to be contacted
    - ❖ Nature of communication
    - ❖ Further requirements to manage any other contact
        - o School contact point / DPO
        - o Other short term contact points for any people that are affected (where loss affects numerous subjects).
- Send notification to any partners affected, e.g. Social Care team.
- Where applicable notify the ICO via the report a breach' page of the ICO website within 72 hours of being notified of the breach. If all 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.

5.0 REMEDIATION

- The DPO will identify any mitigation that prevents a recurrence.
- The Headteacher / Business Manager / Other (specify) will implement any agreed mitigating actions.
    - ❖ This will include any process changes, quality assurance checks or technical controls.

6.0 MONITORING

6.1 Logging

The breach will be logged on the central logging database by the Data Protection Officer.

6.2 Monitoring

The DPO will review actions to:

- Ensure that they have been implemented
- Test that the risk has been minimised/eliminated

6.3 Reporting

A copy of the Data Breach Investigation Report (see Appendix 2) will be provided to the Headteacher/Board of Governors/Trust. A report of breaches will be provided to the Headteacher/Board on a termly basis.

7.0 CLOSURE

The Data Protection Officer will confirm that the incident is closed once satisfied with the remediation plan and that any information required for external organisations such as the ICO is provided.

DATA BREACH DEFINITION POLICY

Introduction

Plymouth High School is the data controller for a large amount of personal data. If any of this information is subject to a data breach, it should be managed according to best practice, as the school will have responsibility for the breach and any consequences with organisations such as the Information Commissioners Office, (ICO).

Breach definition

A breach is defined as:

- Any event where a person gains access to information or data that they are not authorised to access.
    - This includes information in any format, and breaches where someone's job role does not permit them to access specific information.
- Any event where information (or access to information) is lost and cannot be used for its intended purpose by authorised people.
    - This will include information that has been lost, accidentally deleted and cannot be recovered and information that has become corrupt.
- Integrity breaches are defined as any situation where information has been changed by unauthorised people or actions, rendering the information invalid for the intended purpose.
- Any other event which contravenes the Data Protection Act 2018
    - This will include re-identifying people from data which has had personal details changed to conceal the original identity (pseudonymised) & changing data to prevent disclosure.

Breach classification

Breaches are classified in the following manner:

- Sensitive electronic data disclosure
- Sensitive paper information disclosure
- Electronic data disclosure
- Paper information disclosure
- Data disclosure near miss
- Other data disclosure
    - This includes breaches involving conversations and voicemail.
- Third party breach
- Lost sensitive information
    - Both paper and electronic
- Lost non-sensitive information
    - Both paper and electronic
- Integrity threat
- Storing information past the retention date
- Other DPA18 compromise
    - Failure to conduct DPIA

All partners handling information should use the same classifications for clarity. Sensitive information primarily uses the definition included in the Data Protection Act, which includes racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life. However for this purpose also includes information about 'children's services interactions, free school meal status, pupil premium eligibility, elements of special educational need information, safeguarding information and business processes about such data', as there could be a detrimental impact on those affected.

The difference between electronic disclosure and paper disclosure is the format of the information at the time of the breach.

The school also records "Near Miss" events, which is where any data is sent to unauthorised people, however is retrieved before it is accessed. This enables any lessons learnt to be applied, and reduce the number of actual breaches and the impact of breaches as a whole for the organisation.

Breach Management

The best practice breach management process should be used which follows the steps below:

- Identification
    - ❖ The ability to identify a breach. This can be from staff reporting, partner reporting, parent or pupil reporting or other monitoring.
- Containment
    - ❖ Preventing any further disclosure.
    - ❖ Where possible retrieving any lost data.
- Impact analysis
    - ❖ Analysing the breach to determine what the impact will be. This will be an assessment of the impact on the data subject of the particular aspect of the breach.
- Notification
    - ❖ Notification according to internal reporting process
        - For detailed reporting process, please see Appendix 3.
    - ❖ Notification to any data subjects affected.
- Remediation
    - ❖ Identification and implementation of any mitigation that prevents a recurrence.

Escalation points

All breaches must be escalated immediately to the Data Protection Officer and the Headteacher. In cases of electronic breaches the IT manager must also be notified immediately so that they can address any system issues. If the breach involves one of our partners, any breach must be reported to their data protection officer or contract manager.

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 necessary, the breach will be escalated by the Data Protection Officer to the ICO, using the ICO matrix. An example of the matrix for Health and Social care is in Appendix 4, this matrix will be followed by our school unless otherwise instructed. In the case of a cyber-compromise, the National Cyber Security Centre and law enforcement will also be notified.

Closure

The incident can be closed only on agreement with the Data Protection Officer. This will ensure that both parties are satisfied with the remediation plan, and that any information required for external organisations such as the ICO is provided.

APPENDIX 1

DATA BREACH REPORT: Initial Details

This report template is to be used when a data breach occurs or is suspected to have occurred. Please complete the form, (however do not send any sensitive details, all that is needed is that breach has occurred). Then send the form to krogers@phsg.org and swillis@phsg.org

Initial actions

1. If possible, recover the data / document as soon as possible
2. Stop further data loss
3. Consult with a manager
4. Report the incident

Initial details		
1	Date / Time of incident:	Click here to enter a date.
2	School / department / service / teams involved:	
4	Author of this incident report (job title & name):	
5	How many persons were affected?	
6	Was this a 'near miss' or loss?	Near miss / loss

Incident details / Nature of breach
Summary of affected data
Data sensitivity – Select the option which describes the data involved in the breach
Choose an item.
Consequences of the breach
Actions Taken
Have all individuals been informed?

APPENDIX 2

DATA BREACH INVESTIGATION REPORT

Initial details		
1	Date / Time of incident:	
2	Directorate / department / service / teams involved:	
3	ICT reference number:	
4	Author of this incident report (job title & name):	
5	How many persons were affected?	
6	Was this a 'near miss' or loss?	

Incident details / Nature of breach
Summary of affected data
Containment
Impact of data breach
Data sensitivity – Select the option which describes the data involved in the breach?
Choose an item.
Notification

Escalated to ICO	
Root cause	

Remediation
Lessons to implement
Conclusion

Appendix A: (of data breach investigation report)

Timeline	
Date and time	Details

Appendix B:

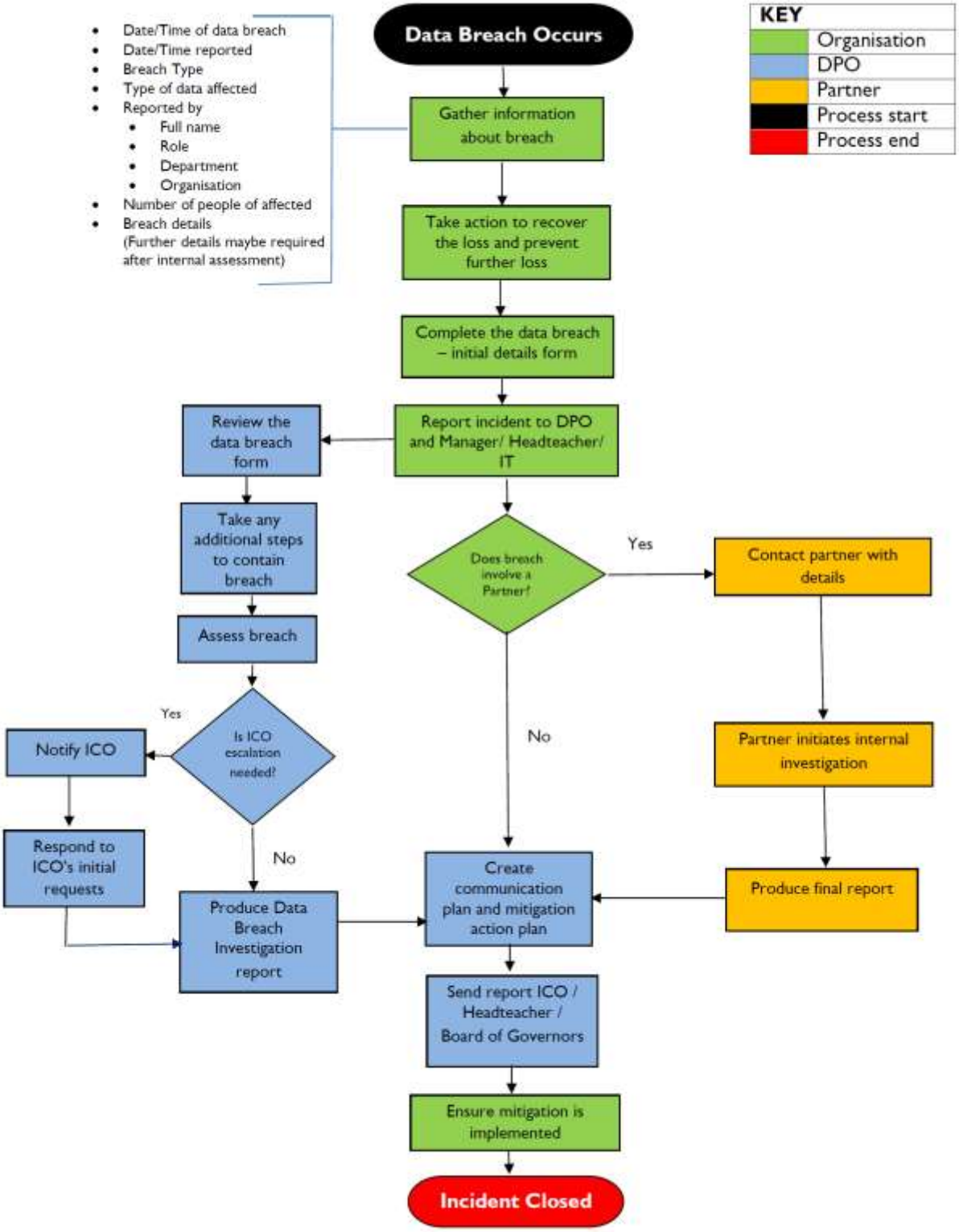
Evidence	
Name	Details

Appendix C: any other information

Form completed by	
Name	Details

APPENDIX 3

Data Breach Reporting Process



APPENDIX 4: ICO escalation matrix for Health and Social Care

Stage No	Risk	Stage	Criteria	Value	Score
1	Low	Scale	Less than 10 individuals	0	
1	Low	Scale	11-50 individuals	1	
1	Low	Scale	51-100 individuals	1	
1	Medium	Scale	101-300 individuals	2	
1	Medium	Scale	301-500 individuals	2	
1	Medium	Scale	501-1000 individuals	2	
1	High	Scale	1001-5000 individuals	3	
1	High	Scale	5001-10,000 individuals	3	
1	High	Scale	10,001-100,000 individuals	3	
1	High	Scale	100,001 + individuals	3	
2	Low	Sensitivity Factor	No sensitive personal data (DPA defintion) at risk nor data to which a duty of confidence is owed	-1	
2	Low	Sensitivity Factor	Information readily accessible or already in the public domain or would be made available under access to information legislation	-1	
2	Low	Sensitivity Factor	Information unlikely to identify individual(s)	-1	
2	High	Sensitivity Factor	Detailed information at risk e.g. clinical/care case notes, social care notes	1	
2	High	Sensitivity Factor	High risk confidential information	1	
2	High	Sensitivity Factor	One or more previous incidents of a similar type in the past 12 months	1	
2	High	Sensitivity Factor	Failure to implement, enforce or follow appropriate organisational or technical safeguards to protect information	1	
2	High	Sensitivity Factor	Likely to attract media interest and/or a complaint has been made directly to the ICO by a member of the public, another organisation or an individual	1	
2	High	Sensitivity Factor	Individuals affected are likely to suffer substantial damage or distress, including significant embarrassment or detriment	1	
2	High	Sensitivity Factor	Individuals affected are likely to have been placed at risk of or incurred physical harm or a clinical untoward incident	1	
			Score Total		
			Calculate the score for every factor that is affected by the breach.		
			If Score is above 2, escalate to ICO		