Date March 2018
Review Date March 2021
Responsibility Bursar

EPSOM
COLLEGE

Data Breech Policy and Procedures
To be used following an actual or suspected data breach

1 Introduction

1.1 The College understands the importance of keeping personal data secure and of effectively dealing with data breaches. This is essential for maintaining the trust of staff, pupils and their parents when the College uses their information.

1.2 This policy and procedure is to be used by the College's Data Breach Response Committee in the event of a data breach at the College (or a suspected data breach). The Committee is comprised of the senior members of staff (named at section 4.1 below) who will deal with different aspects of a data breach.

1.3 All staff should receive training on how to recognise a data breach and the College's Information Security Policy contains guidance for staff on this issue.

1.4 The College is required to report certain breaches to the Information Commissioner's Office (ICO) and to data subjects under the General Data Protection Regulation (GDPR). There are strict timescales for reporting breaches which are outlined in section 7.

1.5 The College also has responsibilities to report certain incidents to other regulators such as the Charity Commission. Section 7 below covers these reporting obligations.

2 Immediate action following a data breach

- Inform all members of the Data Breach Response Committee;
- Identify what personal data is at risk;
- Take measures to prevent the breach from worsening e.g. changing password/access codes, removing an email from pupils' inboxes which was sent by mistake;
- Recover any of the compromised personal data e.g. use back-ups to restore data;
- Consider whether outside agencies need to be informed as a matter of urgency e.g. the police in the event of a burglary or Children's Services where the breach may lead to serious harm being caused to a pupil;
- Consider whether any affected individuals should be told about the breach straight away. For example, so that they may take action to protect themselves or because they would find out about the breach from another source. Please note this is different to the mandatory notification to individuals covered at 7.6 - 7.10 below which does not need to be an immediate notification.

3 What is a data breach?

3.1 A data breach is a breach of security which leads to any of the following:

3.1.1 the loss of personal data;

3.1.2 the accidental or unlawful destruction of personal data;

3.1.3 the disclosure of personal data to an unauthorised third party;

3.1.4 the unlawful or accidental alteration of personal data; or

3.1.5 unauthorised access to personal data.

3.2 Personal data is information:

3.2.1 from which a person can be identified (either from the information itself or when combined with other information likely to be used to identify the person); and

3.2.2 which relates that person.

3.3 The following are examples of personal data held by the College:

3.3.1 names and contact details of pupils, parents and staff;

3.3.2 financial information about parents and staff;

3.3.3 pupil exam results;

3.3.4 safeguarding information about a particular family;

3.3.5 information about pupil behaviour and attainment; and

3.3.6 a pupil or staff member's medical information.

3.4 If staff are in any doubt as to whether an incident constitutes a data breach they must speak to the Bursar or Headmaster immediately.

3.5 Please see Appendix 1 for examples of data breaches.

4 Roles and responsibilities

4.1 The following staff form the College's Data Breach Response Committee (the **Committee**) and will have certain responsibilities:

Role	**Responsibility**
The Bursar	The Bursar will chair the Committee and is responsible for co-ordinating the College's response to any breach. In addition, the Bursar will lead on any physical security measures which are required at the College site to contain the breach. The Bursar is responsible for notifying and liaising with the College's insurers as required.
The Headmaster	The Headmaster will be responsible for any communications with pupils and parents and for any pupil welfare or disciplinary considerations.

The HR Manager	The HR Manager will lead on any employee welfare or disciplinary issues in consultation with the Head.
The Director of Transformation and IT	The Director of Transformation and IT will be responsible for ensuring the security of the College's ICT infrastructure. In addition, for taking any possible technical measures to recover personal data or to contain a data breach.
The Chair of Governors	The Chair of Governors will be responsible for liaising with the Board of Governors as appropriate. Any decision to report the data breach to the Charity Commission will be taken by the Board of Governors.

4.2 The Committee will form as soon as possible once a data breach has been identified.

5 Containment and recovery

5.1 As soon as a data breach has been identified or is suspected, steps must be taken to recover any personal data and to contain the breach. For example, the College may need to:

5.1.1 change any passwords and access codes which may have been compromised;

5.1.2 if appropriate in all the circumstances, tell employees to notify their bank if financial information has been lost (or other information which could lead to financial fraud) and offer credit protection;

5.1.3 limit staff and/or pupil access to certain areas of the College's IT network;

5.1.4 use back-up tapes to restore lost or damaged data;

5.1.5 take any measures to recover physical assets e.g. notifying the police or contacting third parties who may have found the property;

5.1.6 notify its insurers; and

5.1.7 take action to mitigate any loss.

5.2 The Committee should decide what action is necessary and which member(s) of the Committee will be responsible for the different aspects of the containment and recovery. Where appropriate the Committee will delegate tasks to other members of staff with the relevant expertise.

5.3 The Committee should seek assistance from outside experts if appropriate to effectively contain the breach and recover any personal data. For example, legal advice, reputation management advice or specialist technical advice.

6 Establishing and assessing the risks

6.1 The next stage in the process of dealing with a data breach is to establish and assess the risks presented by the breach. To assist with this process, the Committee should document the answers to the questions contained in 0 in as much detail as possible.

6.2 The table in 0 should be copied into a new document in order to retain a record of this process.

7 Notification

Notification to the Information Commissioner's Office

7.1 From 25 May 2018 the College will be required to report a data breach to the ICO unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. The exercise which was documented under section 6 above should be used to determine if a notification to the ICO is required.

7.2 "Risk to the Rights and freedoms of individuals" should be interpreted broadly. Please see row 5 of 0.

7.3 Any decision to not notify the ICO should be documented. It is possible that if another data breach occurs in the future that the ICO will ask why any previous breaches were not reported and the ICO is likely to ask to see evidence of any decision to not notify.

7.4 If the College decides to notify the ICO then this must be done without undue delay and where feasible within 72 hours of having become aware of the breach.

7.5 Content of the notification

7.5.1 The ICO has set out procedures for notifications on their website (ico.org.uk) which should be followed.

(a) However, the College should also prepare a letter to the ICO in addition to following the ICO's procedures on the website in all but the most minor breaches because this provides the opportunity to present what has happened in a way that is advantageous to the College.

(b) The College may need to send this letter after the initial notification to incorporate any subsequent action taken by the College which may act in mitigation against ICO enforcement action.

7.5.2 The notification must contain as a minimum:

(a) a description of the nature of the data breach including where possible:

(i) the categories and approximate number of data subjects concerned; and

(ii) the categories and approximate number of personal data records concerned.

(b) the name and contact details of the Bursar who can provide more information to the ICO if required;

(c) a description of the likely consequences of the data breach;

(d) a description of the measures taken or proposed to be taken by the College to address the data breach, including, where appropriate, measures to mitigate its possible adverse effects.

7.5.3 If it has not been possible to submit the notification to the ICO within 72 hours of becoming aware of the breach, the notification must explain the reason for this delay. For example, that the College has been instructed by the police to postpone the notification to the ICO.

7.5.4 If it is not possible to provide all of the information at the same time, the College should provide the information to the ICO in phases without further undue delay. For example, the College

could make an initial notification within the 72-hour period with a more detailed response the following week once the College has more information on what happened.

7.5.5 The initial notification should include points such as the possible cause of the breach and how the College plans to deal with the breach including mitigation actions.

7.5.6 The more detailed response should set out as clearly as possible the steps the College has taken to prevent a reoccurrence. The ICO is less likely to take enforcement action if it considers that the College has already taken steps to address what went wrong.

Contacting affected individuals

7.6 The College is required by the GDPR to report a data breach to the individuals whose data has been compromised (known as data subjects) where the breach is likely to result in a high risk to the rights and freedoms of individuals. It may not always be clear which individuals should be notified, for example, parents may need to be notified rather than their children.

7.7 The College should use the exercise at section 6 above to assist with this decision. A notification does not need to be made where:

7.7.1 the College had taken measures so that the data compromised was unintelligible to any person not authorised to access it (e.g. it was encrypted); or

7.7.2 the College has managed to contain the breach or take mitigating action so that any high risk to individuals is no longer likely to materialise (e.g. an unencrypted memory stick has been recovered before anyone was able to access the data held on it).

7.8 If the College decides not to notify individuals this decision must be documented.

7.9 If a notification is sent this must be done so without undue delay. The College should work with the ICO in determining when is the most appropriate time to notify the individuals. Other outside agencies, such as the police, may also have a view regarding the timing of this notification.

7.10 The ICO may advise or require the College to notify individuals. In addition, the ICO has the authority to require a more detailed notification to be given to individuals. The ICO is given these powers under the GDPR.

7.11 **Content of the notification to individuals**

7.12 The notification to individuals must include the following as a minimum:

7.12.1 the name and contact details of a person at the College who can provide more information. The Committee should choose the appropriate staff member at the College, which is likely to depend upon which individuals are affected;

7.12.2 a description of the likely consequences of the data breach; and

7.12.3 a description of the measures taken or proposed to be taken by the College to address the data breach, including, where appropriate, measures to mitigate its possible adverse effects.

7.13 In addition, the College must consider if any additional information would be helpful to data subjects. For example, instructions on measures which they can take to protect their data now or in the future.

7.14 The notification must be drafted in clear language. If directed at pupils the notification should be age appropriate.

7.15 The Committee should decide what is the most appropriate method of communication for the notification. Factors to consider include the urgency of the notification. For example, it may be appropriate to telephone individuals followed up with an email.

Serious Incident Report to Charity Commission

7.16 The Charity Commission's guidance makes it clear that serious incidents should be reported to it as soon as possible. Where there has been a data breach, the Governors will need to consider whether to make a serious incident report to the Charity Commission.

7.17 Governors should consider the Charity Commission's guidance on reporting serious incidents and in particular, the examples of what to report in the "Data breaches or loss" section of their table of examples.

7.18 The Charity Commission has extensive information sharing powers with other regulators, like the ICO, so the Commission may be aware if a serious incident report is not made. This does not absolve the Governors of the obligation to make a serious incident report, rather it increases the likelihood of the Commission detecting a failure to do so.

7.19 Because of the breadth of the Charity Commission's criteria for making serious incident reports, Governors should consider whether to make a report in light of the data breach and surrounding circumstances - even where it has not been necessary to notify the ICO.

Notification to the police

7.20 The College should consider whether the police need to be notified about the data breach because it is possible that a criminal offence has been committed. However, there is no legal obligation to notify the police. The following are examples of breaches where a criminal offence may have been committed:

7.20.1 theft e.g. if a laptop has been stolen;

7.20.2 burglary;

7.20.3 if a staff member has shared or accessed personal data where this was not required as part of their professional duties e.g. a staff member shares information about a pupil with famous parents with the local press;

7.20.4 the College's computer network has been hacked (e.g. by a pupil or a third party).

7.21 Action Fraud is the national fraud and cybercrime reporting centre. It can be contacted on 0300 123 2040 or using www.actionfraud.police.uk

8 Internal Breach Register

8.1 The College is required to keep a register of all data breaches including those which do not meet the threshold to be reported. Staff should be trained to report all data breaches to allow the College to meet this requirement.

8.2 The Bursar is responsible for keeping this register up to date.

9 Evaluation

Evaluation of the College's security measures

9.1 The College is obliged under the GDPR to implement technical and organisational measures to protect personal data. The College regularly evaluates of the effectiveness of both its organisational and technical measures.

9.2 Organisational measures include:

9.2.1 policies for staff on their data protection obligations, including when working away from the school site;

9.2.2 guidance for staff on how to use specific computer applications and software securely; and

9.2.3 data protection training for staff.

9.3 Technical measures include:

9.3.1 the use of encryption;

9.3.2 limiting access to certain areas of the College's IT network;

9.3.3 firewalls and virus protection; and

9.3.4 the use of backups.

9.4 The Committee should establish how the existing measures could be strengthened and what additional measures should be put in place to guard against future data breaches. The Committee should consider both breaches of a similar type to that which has occurred and the risk of security breaches more broadly.

9.5 The Committee may delegate this task to one or more appropriate members of staff. The Committee should consider whether legal and/or technical advice is required.

9.6 This exercise should be undertaken promptly because the actions taken by the College to improve its practices will likely be taken into account by the ICO when considering if enforcement action should be taken against the College.

9.7 Key points to consider include:

9.7.1 Would improvements in the training given to staff have prevented the breach or lessened the severity of the breach?

9.7.2 Can measures be taken to speed up the process of staff reporting breaches?

9.7.3 Does the College's Information Security Policy need to be revised?

9.7.4 Are changes required to the College's IT system?

9.7.5 Should the College's document management system be made more robust? For example, should staff's ability to access certain documents be limited to a greater extent?

9.7.6 Does the physical security of the College, particularly in areas where personal data is kept, need to be improved?

9.7.7 Do the College's remote working practices need to change?

9.7.8 Does the College need more robust procedures around staff using their own devices for school work?

9.7.9 Do the College's contracts with processors (e.g. a Cloud storage provider) need to be revised?

9.7.10 Does the College need to do more robust due diligence on its processors?

9.7.11 If any IT services providers were contracted by the College to carry out work related to information security was the service provided adequate?

9.8 The Committee should report the outcome of the evaluation to the Board of Governors before implementing any necessary changes.

Evaluation of the College's response to the data breach

9.9 When the immediate action has been taken following the data breach, the College should evaluate how its initial response to the breach could have been better.

9.10 Key points to consider:

9.10.1 Was the breach reported to the Bursar immediately? If not, what action can be taken to speed up the process of contacting a senior member of staff.

9.10.2 Were all possible measures taken to recover the data promptly?

9.10.3 Could more have been done to contain the breach as quickly as possible?

9.10.4 If one of the College's processors (e.g. a payroll supplier) was either responsible for the breach, or discovered the breach, was this notified to the College without undue delay? If not, what measures can be put in place to improve this communication in the future?

9.11 The Committee should report the outcome of the evaluation to the Board of Governors before implementing any necessary changes.

10 Tactical considerations

10.1 The College should refer to Appendix 4 which outlines tactical and supplemental considerations. For example, is any pupil disciplinary action required?

11 Monitoring and review

11.1 The Bursar should ensure that this policy is regularly reviewed and updated as required.

11.2 This policy should be reviewed following any data breach at the College which meets the threshold to be reported to the ICO.

Appendix 1 Examples of data breaches and the next steps

Example of breach	Containment and Recovery	Establishing and Assessing the Risks	Notification	Evaluation of the College's response to the data breach
A staff member leaves papers containing information about pupils' academic performance on a train. The papers were not in a locked case.	The College should find out if it is possible to retrieve the papers. For example, by calling the train company's lost property department.	The College should work through the questions in 0 below.	If the papers are not retrieved then this breach will need to be notified to the ICO. Whether a notification to the pupils and their parents is required will depend upon the nature of the personal data. The College should consult section 7 of this policy.	The College should work through sections 9.9 to 9.11 of the policy above.
Ransomware locks electronic files containing personal data.	The College should have a back-up of the data and should also ensure that its systems are secured (e.g. that the ransomware has been removed).	Ditto	Depends on factors such as whether the College was able to recover the data and whether there is any other risk to the College's systems	Ditto
Sending an email containing personal data to the incorrect recipient.	Use the recall email feature if available. Consider calling the unintended recipient and asking them to delete the email	Ditto	Depends on the sensitivity of any personal data contained in the email, whether the unintended recipient has agreed to delete it etc.	Ditto

Appendix 2 Establishing and Assessing the Risks Presented by the Data Breach

	Question	**Response**
1.	Precisely what data has been (or is thought to have been) lost, damaged or compromised?	
2.	Is any of the data Critical Personal Data as defined in the College's Data Protection Policy for Staff? This would be: i. information concerning child protection matters; ii. information about serious or confidential medical conditions and information about special educational needs; iii. information concerning serious allegations made against an individual (whether or not the allegation amounts to a criminal offence and whether or not the allegation has been proved); iv. financial information (for example about parents and staff); v. information about an individual's racial or ethnic origin; and vi. political opinions; vii. religious beliefs or other beliefs of a similar nature; viii. trade union membership; ix. physical or mental health or condition; x. genetic information; xi. sexual life; xii. information relating to actual or alleged criminal activity; and xiii. biometric information (e.g. a pupil's fingerprints following a criminal investigation). If any of these types of data are involved this makes the breach more serious.	
3.	Who are the affected individuals e.g. staff, parents, pupils, third parties?	

4.	How many individuals have definitely been affected and how many potentially affected in a worst-case scenario?	
5.	What harm might be caused to individuals (not to the College)? The individuals do not necessarily need to be those whose personal data was involved in the breach. Harm should be interpreted broadly, for example to include: (a) distress; (b) discrimination; (c) loss of confidentiality; (d) financial damage; (e) identity theft; (f) physical harm; and (g) reputational damage.	
6.	What harm might be caused to the College? For example, reputational damage and financial loss.	
7.	What mitigating factors may have lessened the risks presented by the breach? The following questions may assist when considering this point. (a) Were any physical protections in place to limit the impact of the breach e.g. was the data contained in a locked case when it was lost/stolen? (b) Were any technical protections in place e.g. was the data protected by encryption? (c) Have measures been taken to contain the breach e.g. have banks being notified where financial information has been compromised? (d) Have measures been taken to recover the data e.g. has lost data been found before being seen by any unauthorised party or have back-ups been used where electronic information was lost or damaged?	

Appendix 3 External advice

Legal advice

The College should consider taking legal advice in relation to the following. Please note that this is not an exhaustive list but should be used as a guide.

1. Determining whether to notify the ICO and the data subjects.
2. Drafting the notification to the ICO and the data subjects.
3. Drafting a serious incident report to the Charity Commission.
4. Any correspondence with other external agencies such as the Independent Schools Inspectorate or the Department for Education.
5. Any communications with the police.
6. The decision to notify the College's insurers.
7. Any communications with staff members, pupils and parents.
8. Any disciplinary action in relation to pupils or staff.
9. Establishing whether there is a risk that an affected individual might bring a legal claim against the College.

Reputation management

The College should consider obtaining advice regarding reputation management. This advice may be provided by solicitors or by other specialists. As above, this is not an exhaustive list but should be used as a guide.

The following circumstances in particular may require specialist advice:

1. If the data breach becomes widely known to the parental community.
2. If news of the breach becomes known outside of the College community.
3. If the media report on the breach or ask the College for a statement.
4. If the ICO take enforcement action which may become public knowledge.

Appendix 4 Tactical and supplemental considerations

This appendix should be completed to assist the College in checking that all issues surrounding the data breach have been considered. It is not an exhaustive list but may assist the Committee when handling the consequences of the data breach.

Supplemental issue	**Considerations**
Pupil welfare	
Staff welfare	
Parental complaints	
Staff disciplinary action	
Pupil disciplinary action	
Reputation management	
Risks of legal claims	
Possible Charity Commission action	