Title:	**Personal Data Breach Notification Policy**
Reviewed by:	**Data Protection Officer**
Approved by:	**SMT**
Date of review:	**May 2019**
Date of next review:	**May 2021**
Associated documents/policies:	• Personal Data Breach Notification Procedure • Data Protection Policy • Retention of Records Policy • Rights of Individuals Policy • Information Security Policy • Confidentiality Policy

TABLE OF CONTENTS

1. OVERVIEW

1.1. The College's reputation and future growth are dependent on the way the College manages and protects Personal Data. As an organisation that collects, holds, shares and uses Personal Data, the College takes seriously its obligations to keep that Personal Data secure and to deal with security breaches relating to Personal Data when they arise.

1.2 The College's key concern in relation to any breach affecting Personal Data is to contain the breach and take appropriate action to minimise, as far as possible, any adverse impact on any individual affected. The College has therefore implemented this Policy to ensure all College Personnel are aware of what a Personal Data breach is and how they should deal with it if it arises.

- Every care is taken to protect personal data from incidents (either accidental or deliberate) to avoid a data protection breach that could compromise security.

- This Policy does not form part of any College member of staff's contract of employment and the College reserves the right to change this Policy at any time. All College members of staff are obliged to comply with this Policy at all times.

2. ABOUT THIS POLICY

2.1 This Policy explains how the College complies with its obligations to recognise and deal with Personal Data breaches and (where necessary) to notify the ICO and the affected individuals. The College has a corresponding Data Breach Notification Procedure and Data Breach Register that set out how the College deals with and records Personal Data breaches.

3. SCOPE

3.1 This Policy applies to all staff, including temporary, casual or agency staff, and contractors, consultants, suppliers and data processors working for, or on behalf of the College who collect and/or use Personal Data relating to individuals.

3.2 It applies to all personal data held by the College stored electronically, in paper form, or otherwise.

3.3 This policy sets out the process to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents across the College.

3.4 The objective of this policy is to contain any breaches, to minimise the risk associated with the breach, consider what action is necessary to secure personal data and prevent further breaches.

4. DEFINITIONS

- **College** – Bath College.

- **College Personnel** – Any College employee or contractor who has been authorised to access any of the College's personal data and will include employees, consultants, contractors, and temporary personnel hired to undertake work on behalf of the College.

- **Data Protection Laws** – The General Data Protection Regulation (Regulation (EU) 2016/679) and all applicable laws relating to the collection and use of Personal Data and privacy and any applicable codes of practice issued by a regulator including in the UK, the Data Protection Act 2018.

- **Data Protection Officer** – The Data Protection Officer is currently the Principal & Chief Executive , and can be contacted at: telephone 01225 328733 or e-mail dataprotection@bathcollege.ac.uk.

- **ICO** – the Information Commissioner's Office, the UK's data protection regulator.

- **System Owner** – The member of college personnel responsible for the specific College Information System e.g. the Head if Information Systems for the Student Records System or the Head of Finance for the Finance system.

- **Personal Data** – any information about an individual which identifies them or allows them to be identified in conjunction with other information that is held. Personal data is defined very broadly and covers both ordinary personal data from personal contact details and business contact details to special categories of personal data such as trade union membership, genetic data and religious beliefs. It also covers information that allows an individual to be identified indirectly for example an identification number, location data or an online identifier.

- **Special Categories of Personal Data -** Personal Data that reveals a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data (i.e. information about their inherited or acquired genetic characteristics), biometric data (i.e. information about their physical, physiological or behavioural characteristics such as facial images and fingerprints), physical or mental health, sexual life or sexual orientation and criminal record.

5. WHAT IS A PERSONAL DATA BREACH?

5.1 The College takes information security very seriously and the College has security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data. The College has in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction.

5.2 Personal Data breach is defined very broadly and is effectively any failure to keep Personal Data secure, which leads to the accidental or unlawful loss (including loss of access to), destruction, alteration or unauthorised disclosure of Personal Data. Whilst most Personal Data breaches happen as a result of action taken by a third party, they can also occur as a result of something someone internal does.

5.3 An incident, in the context of this policy, is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to the College's information assets and/or reputation.

5.4 A Personal Data breach could include any of the following:

- loss or theft of Personal Data or equipment that stores Personal Data (e.g. loss or laptop, USB stick, iPad/tablet device, or paper record);

- loss or theft of Personal Data or equipment that stores the College's Personal Data from a College supplier;
- inappropriate access controls meaning unauthorised College Personnel can access Personal Data;
- any other unauthorised use of or access to Personal Data;
- deleting Personal Data in error;
- human error (which could be as simple as putting a letter in the wrong envelope or leaving a phone or laptop containing Personal Data on a train);
- hacking attack;
- infection by ransom ware or any other intrusion on our systems/network;
- 'blagging' offences where information is obtained by deceiving the organisation who holds it; or
- destruction or damage to the integrity or accuracy of Personal Data.

5.5 A Personal Data breach can also include:

- equipment or system failure that causes Personal Data to be temporarily unavailable;
- unforeseen circumstances such as a fire, flood or power failure that causes Personal Data to be temporarily unavailable;
- inability to restore access to Personal Data, either on a temporary or permanent basis; or
- loss of a decryption key where Personal Data has been encrypted because this means the College cannot restore access to the Personal Data.

6 REPORTING A PERSONAL DATA BREACH

6.1 College Personnel must immediately notify any Personal Data breach to the Data Protection Officer (dataprotection@bathcollege.ac.uk.) and ICT Services (ICTSupport@bathcollege.ac.uk no matter how big or small and whether or not College Personnel think a breach has occurred or is likely to occur. This allows the College to contain the breach as soon as possible and to consider a recovery plan to minimise any risk of damage to the individuals affected and to the College.

6.2 If College Personnel discover a Personal Data breach outside working hours, College Personnel must notify it to the College's Data Protection Officer and ICT Services as soon as possible.

6.3 The report must include as much information as is available, and preferably full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information and how many individuals are involved. An Incident Report Form should be completed as part of the reporting process (see Appendix 1).

6.4 College Personnel should be aware that any breach of Data Protection legislation or failure to report a data breach may result in the College's Disciplinary procedures being instigated.

6.5 College Personnel may be notified by a third party (e.g. a supplier that processes Personal Data on the College's behalf) that they have had a breach that affects College Personal Data. College Personnel must notify this breach to the College's Data Protection Officer and the College's Data Breach Notification Procedure shall apply to the breach.

7 MANAGING A PERSONAL DATA BREACH

7.1 There are four elements to managing a Personal Data breach or a potential one and this Policy considers each of these elements:

7.1.1 Containment and recovery

7.1.2 Assessment of on-going risk

7.1.3 Notification

7.1.4 Evaluation and response

7.2 At all stages of this Policy, the Data Protection Officer and managers will consider whether to seek external legal advice.

7.3 The Data Protection Officer will also complete the Personal Data Security Breach log, which is the College's Data Breach Register.

7.4 An activity log of all decisions and action taken will be kept by the Data Protection Officer and updated as appropriate.

8 CONTAINMENT AND RECOVERY

8.1 An initial assessment of the Personal Data breach will be carried out either by the Data Protection Officer; by ICT Services; or by the System owner to establish the severity of the breach, and whether the breach is still occurring.

8.2 If the Personal Data breach is unlikely to result in a risk to the rights and freedoms of the individuals affected, then it will be added to the College's Data Breach Register and no further action will be taken.

8.3 If the Personal Data breach may impact on the rights and freedoms of the individuals affected, then the College will put together and implement a bespoke Personal Data breach plan to address the breach concerned in accordance with the College's Data Breach Notification Procedure. This will include consideration of:

8.3.1 whether there are any other people within the College who should be informed of the breach, such as IT team members, to ensure that the breach is contained;

8.3.2 what steps can be taken to contain the breach, recover the loss of any Personal Data or to prevent damage being caused; and

8.3.3 whether it is necessary to contact other third parties such as students, parents, banks, the ICO or the police particularly in the case of stolen Personal Data. All notifications shall be made by the Data Protection Officer or a person nominated by them.

8.4 All actions taken in relation to a Personal Data breach will be in accordance with the Data Breach Notification Procedure which is maintained and administered by the Data Protection Officer.

8.5 The Data Protection Officer is responsible for ensuring that the Data Breach Register is updated.

9 ASSESSMENT OF ONGOING RISK

9.1 As part of the College's response to a Personal Data breach, once the breach has been contained the College will consider the on-going risks to the organisation and to any other party caused by the breach and what remedial action can be taken to minimise the impact of the breach. This will be undertaken in accordance with the College's Data Breach Notification Procedure.

This will take into account the following:

- the type of data involved
- its sensitivity
- the protections in place (e.g. encryptions)
- what has happened to the data (e.g. has it been lost or stolen)
- whether the data has been put to any illegal or inappropriate use
- data subject(s) affected by the breach, number of individuals involved and the potential effect(s) on those data subjects
- whether there are wider consequences to the breach
- the potential for further breaches e.g. in teams operating in a similar way to that experiencing the breach

10 NOTIFICATION

10.1 Under Data Protection Laws, the College *may* have to notify the ICO and also possibly the individuals affected about the Personal Data breach.

10.2 Any notification will be made by the Data Protection Officer or (in the absence of the Data Protection Officer), a person nominated by the Principal & Chief Executive, following the College's Data Breach Notification Procedure. The notification shall comply with the requirements of the ICO. The ICO request that potential data breaches are, during office hours, notified by telephone, and outside of working hours by completion of a personal data breach form.

10.3 Notification of a Personal Data breach must be made to the ICO without undue delay and where feasible within **72 hours of** when the College becomes aware of the breach unless it is '*unlikely to result in a risk to the rights and freedoms of individuals'*. It is therefore imperative that College Personnel notify all Personal Data breaches to the Data Protection Officer; ICT Services and the System Owner immediately.

10.4 Notification of a Personal Data breach must be made to the individuals affected without undue delay where the breach is '*likely to result in a high risk to the rights and freedoms of individuals'*.

10.5 Please note that not all Personal Data breaches are notifiable to the ICO and/or the individuals affected and the College will decide whether to notify and who to notify in accordance with the Data Breach Notification Procedure.

10.6 Where the Personal Data breach relates to a temporary loss of availability of the College's systems, the College does not have to notify if the lack of availability of Personal Data is unlikely to result in a risk to the rights and freedoms of individuals. The College does not consider that it has any systems where temporary unavailability would cause a risk to the rights and freedoms of individuals but this will be assessed on a case-by-case basis in accordance with the Data Breach Notification Procedure.

10.7 In the case of complex breaches, the College may need to carry out in-depth investigations. In these circumstances, the College will notify the ICO with the information that it has within 72 hours of awareness and will notify additional information in phases. Any delay in notifying the ICO must be seen as exceptional and shall be authorised in accordance with the Data Breach Notification Procedure.

10.8 Where a Personal Data breach has been notified to the ICO, any changes in circumstances or any relevant additional information which is discovered in relation to the Personal Data breach shall also be notified to the ICO in accordance with the Data Breach Notification Procedure.

10.9 Where a Personal Data breach has been notified to the ICO, the Data Protection Officer, or, in their absence, the person who notified the ICO, must inform the Head of Governance, who will then inform the Chair of the Corporation and the Chair of the Audit Committee. Both the Chair of the Corporation and the Chair of the Audit Committee should be updated once any correspondence from the ICO is received.

10.10 When the College notifies the affected individuals, it will do so in clear and plain language and in a transparent way. Any notifications to individuals affected will be done in accordance with the Data Breach Notification Procedure. Any notification to an individual should include details of the action the College has taken in relation to containing the breach and protecting the individual. It should also give any advice about what they can do to protect themselves from adverse consequences arising from the breach.

10.11 The College may not be required to notify the affected individuals in certain circumstances as exemptions apply. Any decision whether to notify the individuals shall be done in accordance with the Data Breach Notification Procedure and shall be made by the Data Protection Officer.

11 EVALUATION AND RESPONSE

11.1 It is important not only to investigate the causes of the breach but to document the breach and evaluate the effectiveness of the College's response to it and the remedial action taken.

11.2 There will be an evaluation after any breach of the causes of the breach and the effectiveness of the College's response to it. All such investigations shall be carried out in accordance with the Data Breach Notification Procedure and will be recorded on the Personal Data Breach Register.

11.3 Any remedial action such as changes to the College's systems; policies or procedures will be implemented in accordance with the Data Breach Notification Procedure.

12 MONITORING & INTERNAL REPORTING

12.1 Personal Data breaches will be reported to the first SMT meeting following the data breach and SMT will be updated from the investigation as appropriate.

12.2 A report will be presented to each Audit Committee meeting, outlining any Personal Data breaches or nil returns.

Appendix 1

DATA BREACH REPORT FORM

Please act promptly to report any data breaches. If you discover a data breach, please immediately complete Section 1 of this form and email it as soon as possible to the Data Protection Officer (dataprotection@bathcollege.ac.uk) and ICT Helpdesk (ictsupport@bathcollege.ac.uk).

Section 1: Notification of Data Security Breach	To be completed by person reporting the incident
Date incident/breach was discovered:	
Date(s) of incident/breach:	
Name of person reporting the incident:	
Contact details of person reporting the incident:	
Brief description of the incident and/or details of the information lost:	
Details of the IT system, equipment, devices, records involved in the security breach:	
Is the data bound by any contractual security arrangements?	
Is the data owned by the College or is it owned by an external body?	
Has the breach occurred within the College or have we been notified of a breach of our data by a third party?	
Number of data subjects affected, if known:	
Brief description of any action taken at the time of discovery:	
Is the information unique? Will its loss have adverse operational, financial, legal liability or reputational consequences for the College or third parties?	
Was the Personal Data backed up onto central ICT systems?	
What are the potential consequences (if known) of the breach?	

Categories of Personal Data included in the breach:

☐Data Revealing racial or ethnic origin
☐Political opinions
☐Religious or philosophical beliefs
☐Trade union membership
☐Sex life data
☐Sexual orientation data
☐Gender reassignment data
☐Health data
☐ Performance data (appraisals, grades, discipline cases)
☐Salary data
☐Basic personal identifiers (name, contact details, date of birth, NI number etc.)
☐Identification data (usernames, passwords etc.)
☐Economic and financial data (credit card numbers, bank details, etc.)
☐Official documents (driving licences, passport copies etc.)
☐Location data
☐Genetic or biometric data
☐Criminal convictions/offences
☐Not yet known
☐ Other

If other, please give details below:

Categories of data subjects affected:

☐Employees
☐Students
☐Customers or prospective customers
☐Children
☐Vulnerable adults
☐Vulnerable children
☐Not yet known
☐Other

If other, please give details below:

Type of breach:

☐Device lost/stolen (encrypted)
☐Device lost/stolen (unencrypted)
☐ Hacking
☐Inappropriate disposal of paper
☐Malware
☐Paper lost or stolen
☐Phishing
☐Other

If other, please give details below:

For use by Data Protection Officer/ICT Services	
Received by (name):	
On (date):	
Forwarded for action to (name):	
On (date)	