BRIDGWATER & TAUNTON COLLEGE

PERSONAL DATA BREACH POLICY AND PROCEDURE

(previously known as Data Security Incident Management Policy)

Effective for all staff, students, visitors and contractors

Author:	Information Systems & Exams Manager
Approved by:	SMT
Date:	May 2018
Revised:	November 2018
Review date:	November 2020

Contents

1 Introduction

1.1 The General Data Protection Regulation (GDPR) regulates the processing of personal data by the College. The College will make all reasonable endeavours to ensure that there are no personal data breaches.

1.2 A personal data breach is defined as “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.” The cause of which can be accidental, or deliberate. This definition means that a breach is about more than just the loss of personal data. Every care is taken to protect personal data from incidents (either accidental or deliberate) to avoid a data breach that could compromise security.

A compromise of information, confidentiality, integrity or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative non-compliance and/or financial penalties.

1.3 The College 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 information assets as far as possible.

1.4 For the purpose of this policy, data security breaches include both confirmed and suspected incidents.

1.5 Types of incident include, but are not restricted to::

- Loss of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad, tablet device or paper record)
- Careless document storage, display or retention leading to confidential personal data being visible to others on screen or on paper
- Equipment theft or failure
- System failure
- Unauthorised use of, access to or modification of data on information systems
- Attempts (failed or successful) to gain unauthorised access to information on IT system(s)
- Unauthorised disclosure of sensitive / confidential data
- Website defacement
- Hacking attack
- Unforeseen circumstances such as fire or flood
- Human error
- ‘Blagging’ offences where information is obtained by deceiving the organisation who holds it

2 Aim of the Policy

2.1 The aim of this policy is to standardise the College’s response to any reported data breach, ensure they are appropriately logged and managed in accordance with best practice guidelines, ensure any breaches are contained, risks associated with the breach minimised and actions considered to secure personal data and prevent further breaches.

2.2 This policy applies to all College information, regardless of format, and applies to all staff, students, visitors and contractors acting on behalf of the College.

2.3 By adopting a consistent approach to all reported incidents it will ensure that:

- Incidents are reported in a timely manner and can be properly investigated
- Incidents are managed by appropriately authorised and skilled staff
- Appropriate levels of College management are involved in response management
- Incidents are recorded and documented
- The impact of an incident is understood and action is taken to prevent further damage
- Evidence is gathered, recorded and maintained in a form that will withstand both internal and external scrutiny
- As appropriate, data subjects or external bodies are informed
- Timely management of incidents with minimal disruption to operation
- Incidents are reviewed to identify policy or procedural improvements.

3 Responsibilities

3.1 Information users are responsible for reporting actual, suspected, threatened or potential information security incidents and for assisting with investigations as required, particularly where urgent action is needed to prevent further damage.

3.2 Assistant Principals and Directors are responsible for ensuring that staff in their area act in compliance with this policy and assist with investigations as required.

3.3 The Principal will be responsible for overseeing management of the breach in accordance with the Data Breach Management Plan. Delegation may be appropriate in some circumstances.

4 Data Classification

4.1 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 College is able to quickly identify the classification of the data and respond to all reported incidents in a timely and appropriate manner.

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

Public – any information published or available publicly (in the public domain)
Internal – any information circulated within the College only, including information which is only accessible to certain employees/groups/committee members/contracted parties
Confidential – any personal or confidential information
Protected – highly sensitive information.

5 Data Security Breach Reporting

5.1 Confirmed or suspected data security breaches should be immediately reported to the Data Protection Officer (dpo@btc.ac.uk). Under the GDPR any confirmed or suspected data security breaches must be reported to the ICO within 72 hours (non-working hours) of the College becoming aware of the incident. In the event it is not possible to investigate a breach fully within 72 hours, the DPO will report as much

information as possible, explaining the delay and submit further information as soon as possible. The DPO will give the investigation adequate resources and expedite the process as a matter of priority.

5.2 The report to the ICO must include full and accurate details of the incident including who is reporting the incident and what classification of data is involved. This information will include:

- A description of the breach including where possible the categories and approximate number of individuals concerned
- The categories and approximate number of personal data records accessed
- The name and contact details of the DPO
- A description of the likely consequences of the breach
- A description of the measures taken, or proposed to be taken, including where appropriate the measures taken to mitigate any possible adverse effects

The Data Breach Incident Report Form (Appendix 1) must be completed as part of the reporting process.

5.3 Once a data breach has been reported an initial assessment will be made to establish the severity of the breach and who will be responsible for managing the incident (Appendix 2).

The incident will be investigated to determine whether a breach has occurred, by establishing whether personal data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people

5.4 The investigating manager will consider the likelihood and severity of the resulting risk. If there is a likely risk then the DPO will notify the ICO. If the risk is unlikely then the incident will be documented but not reported. This will be judged on a case-by-case basis. To decide, 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) through:

- Loss of control over their data
- Discrimination
- Identity fraud or theft
- 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

5.5 The breach will be documented, irrespective of whether the breach is reported to the ICO. For each breach this will include the:

- The facts and cause of the breach

- Any effects thereof
- Action taken to minimise the breach and ensure as practicably as possible that it does not happen again (such as establishing more robust processes or providing further training for individuals)

The Breach and Near Miss Log will be stored on the College's network, with restricted access.

6 Data Breach Management Plan

6.1 The management response to any reported data security breach will involve the following elements. See the Data Breach Checklist (Appendix 3).

a. Containment and Recovery
b. Assessment of Risk
c. Consideration of Further Notification
d. Evaluation and Response

6.2 Each of these elements will be conducted in accordance with the Data Breach Checklist. An activity log recording the timeline of the incident management will also be completed (Appendix 4).

6.3 If a breach is likely to result in a high risk to the rights and freedoms of individuals, the DPO will notify those affected without undue delay. This will help them to take any necessary steps to protect themselves from the effects of a breach. The notification will include:

- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

6.4 The College will ensure staff are aware of the possible consequences of any data breach and aware of, and conform to, good practice which reduces the likelihood of data breaches occurring.

Governors will be informed of any data breaches on an annual basis, or sooner where a significant breach has occurred.

7 Review of Policy

7.1 The Data Security Incident Management Policy and Procedure will be reviewed in line with future legislative changes, case law or at no later than 2 years after the issue date.

7.2 The planned review date for the Data Security Incident Management Policy and Procedure is every 2 years or in line with legislative changes.

Appendix 1 Data Breach Incident Report Form

Description of the data breach	
Date and time breach was identified	
Name of the person who identified the breach	
Name of the person reporting the breach	
Contact details Telephone/Email	
Classification of data breached **a. Public** **b. Internal** **c. Confidential** **d. Protected**	
Volume of data involved	
Confirmed or suspected breach?	
Is the breach contained or on-going?	
If on-going, what actions are being taken to recover the data?	
Who has been informed of the breach?	
Evaluation of incident severity	
Any other relevant information	

Email this form to: dpo@btc.ac.uk

Received by	
Date/Time	

Appendix 2 Evaluation of Incident Severity

Highly Critical: Major Incident	Contact
• Special category data/sensitive information • Breach involves > 1000 individuals • External third party data involved • Significant or irreversible consequences • Likely media coverage • Immediate response required regardless of whether it is contained or not • Requires significant response beyond normal operating procedures	Incident Lead: Principal Other contacts: Other Senior Management Team (SMT) members as required External parties such as police, Information Commissioner's Office (ICO), individuals affected
Moderately Critical: Serious Incident	**Contact**
• Confidential data/information • Not contained within the College • Breach involves > 100 individuals • Significant inconvenience will be experienced by individuals impacted • Incident may not yet be contained • Immediate response not required • Incident response may require notification to SMT	Incident Lead: Principal (who may wish to delegate to other SMT members or Head of Department (HOD)) Other contacts: Other SMT members as required
Not Critical: Minor Incident	**Contact**
• Internal or confidential data/information • Breach involves < 100 individuals • Risk to College low • Inconvenience may be experienced by individuals impacted • Loss of data/information is contained/encrypted • Incident can be responded to within working hours	Incident Lead: Principal (who may wish to delegate to other SMT or HOD) Other contacts: Other SMT members as required

Appendix 2 Data Breach Checklist

Step	Action	Notes
A	**Containment and recovery**	**To contain any breach, to limit further damage as far as possible and to seek to recover any lost data**
1	Data Protection Officer to ascertain the severity of the breach and determine if any personal data is involved	See Appendix 2
2	Data Protection Officer to forward Data Breach Incident Report Form to Principal	To oversee full investigation and produce report. If personal data has been breached contact the ICO as appropriate.
3	Identify the cause of the breach and whether it has been contained Ensure that the possibility of any further data loss is removed or mitigated as far as possible	Establish what steps can or need to be taken to contain the breach from further data loss. Contact all cross-College teams who can assist in this process. This may involve actions such as taking systems off-line or restricting access to systems to a limited number of staff until more is known about the incident.
4	Determine whether anything can be done to recover any losses and limit any damage that may be caused	Such as physical recovery of data/equipment or where corrupted through use of back-ups.
5	Where appropriate, the Principal to inform the police	Such as in the case of stolen property, fraudulent activity, offence under the Computer Misuse Act
6	Ensure all key actions and decisions are logged and recorded on the timeline	
B	**Assessment of Risk**	**To identify and assess the on-going risks that may be associated with the breach**
7	What type and volume of data is involved?	Data classification/volume of individual data etc.
8	How sensitive is the data?	Sensitive personal data?
9	What has happened to the data?	For example if the data has been stolen, it could be used for purposes which are harmful to the individuals to whom it relates; if damaged this poses a different type and level of risk
10	If the data was lost/stolen, were there any measures in place to prevent access/misuse?	For example encryption of the data or device

11	If the data was damaged/corrupted/lost, were there measures in place to mitigate the impact of the loss?	For example being part of a back-up strategy
12	How many individuals' personal data are affected?	
13	Who are the individuals whose data has been compromised?	Students, applicants, staff, customers, service users or suppliers
14	What could the data tell a third party about the individual? Could it be misused?	Consider this regardless of what has happened to the data.
15	Is there actual/potential harm that could come to any individuals?	For example are the risks to: Physical safety Emotional wellbeing Reputation Finances Identity Or a combination of these and other private aspects of their life
16	Are there wider consequences to consider?	Is there a risk to public health or loss of public confidence in the College?
17	Are there others who might advise on risks/courses of action?	For example if bank account details have been lost, consider contacting the banks themselves for advice on anything they can do to help prevent fraudulent use.
C	**Consideration of Further Notification**	**Notification is to enable individuals who may have been affected to take steps to protect themselves or allow the regulatory bodies to perform their functions**
18	Are there any legal, contractual or regulatory requirements to notify?	For example terms of funding, contractual obligations
19	Can notification help the College meet it's security obligations under the GDPR?	Prevent any unauthorised access, use or damage to the data or loss of it.
20	Can notification help the individual?	Could individuals act on the information provided to mitigate risks (e.g. by changing their password or monitoring their account)?
21	If a large number of people are affected or there are very serious consequences, inform the ICO	
22	Consider the dangers of 'over notifying'	Not all incidents will warrant notification – take a pragmatic approach to notification

23	Consider who needs to be notified, what you will tell them and how this will be communicated	Always consider the security of the medium of communication as well as the urgency. Include a description of how and when the breach occurred and what data was involved. Include details of what has already been done to respond to the risks posed by the breach. Give specific and clear advice to individuals on the steps they can take to protect themselves and how the College can help them. Provide a way for them to contact us for further information or to ask questions about what has happened (e.g. a contact name, helpline number or a web page).
24	Consult the ICO guidance on when and how to notify it about breaches	Where there is little risk that individuals would suffer significant detriment, there is no need to report. There should be a presumption to report to the ICO where a large volume of personal data is concerned and there is a real risk of individuals suffering some harm. Cases should be considered on their own merit and there is no precise definition of what constitutes a large volume of personal data. Guidance available from: https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/
25	Consider, as necessary, the need to notify any third parties who can assist in helping or mitigating the impact on individuals	e.g. police, insurers, professional bodies, trade unions, website/system providers, bank/credit card companies.
D	**Evaluation and Response**	**To evaluate the effectiveness of the College's response to the breach**
26	Establish where any present or future risks lie	
27	Consider the data and contexts involved	What data is held, its extent, sensitivity, where and how it is stored, how long it is kept.
28	Consider and identify any weak points in existing security measures and procedures	In relation to methods of storage and/or transmission, use of storage devices, levels of access, system/network protection.
29	Consider and identify any weak points in levels of security awareness/training	Fill in any gaps through training or specific advice.
30	Report on findings and implement recommendations	Report to SMT/Governors.

Appendix 4 Timeline of Incident Management

Date	Time	Activity	Decision	Authorised by