Procedure for
Assessing and Reporting Data Breaches

Date approved:	7 December 2021
Approved by:	AMT
Responsible Manager (s):	Data Protection Officer
Executive Lead:	Vice Principal Finance and Planning

Applicable to employees:	Yes
Applicable to students:	Yes
Accessible to students:	Yes
Accessible to general public (including clients)	Yes

Consultation

Consultation undertaken with:		Date:
SMT	No	N/A
AMT	Yes	07.12.2021
CCMT	Yes	01.12.2021
Students	No	N/A
Employee representatives ***(HR policies only)***		N/A
Other	No	N/A

Policy review frequency, normally: every 3 years

Contents

1. Scope and purpose of procedure

1.1 Background

The UK General Data Protection Regulation (UK GDPR) requires B&FC to have in place appropriate procedures for the handling of security incidents involving Personal Data. This procedure provides a framework to facilitate compliance with the UK GDPR and to ensure that information is handled correctly and protected from unauthorised access, loss, damage and destruction.

1.2 Purpose

1.2.1 The purpose of an incident response is to ensure:

- That personal-data breaches including potential personal data breaches are detected, reported, categorised and monitored in a consistent manner
- Appropriate assessment of and response to any breach or potential breach
- That serious breaches are reported to the Information Commissioner's Office (ICO) pursuant to the UK GDPR
- Appropriate action is taken to minimise the impact of disclosure
- Appropriate changes are made or training delivered to prevent any repeat incidents

1.3 Intended Audience

1.3.1 The intended audience for this document is employees, students, suppliers, contractors, representatives and partners of B&FC.

1.3.2 All B&FC employees must complete the annual mandatory data protection training course in order to have a broad understanding of the key aspects of privacy legislation and data protection Appropriate additional reading would be

- B&FC Data Protection Policy
- B&FC Data Protection Code of Practice
- B&FC Procedure for Assessing the Need for and Performing Privacy Impact Assessment (PIAs)
- B&FC Clean Desk and Clear Screen Policy
- B&FC Clean Desk and Clear Screen Procedure
- B&FC Information Sharing Code of Practice

1.4 Scope

1.4.1 This procedure applies to all employees, students, suppliers, contractors, representatives and partners of B&FC who process or come into contact with any personal data for which B&FC

- is the data controller
- is the data processor, or
- has an interest in the personal data processed

1.4.2 All employees have a role to play in ensuring the safety and security of personal data they come into contact with and in protecting those data from misuse.

1.5 Terminology

1.5.1 In line with International Organisation for Standardisation (ISO) directive on the use of terminology in standards, and for the avoidance of doubt, the following words have the specific meanings ascribed below when used in this document:

- 'Shall' or 'Must' denote a mandatory requirement. Deviation from these constitutes non conformance
- 'Shall Not' or 'Must Not' denotes something that is prohibited
- 'Should' denotes a recommendation that is non mandatory
- 'Should Not' denotes something that is not recommended
- 'May' denotes something that is optional.

2. Procedure

2.1 Incident Management

2.1.1 A data protection breach is the result of an event or series of events where Personally Identifiable Information (PII) is exposed to unauthorised or

inappropriate processing that results in its security being compromised. The extent of damage or potential damage caused will be determined by the volume, sensitivity and exposure of the PII.

2.1.2 Breach management is concerned with detecting, reporting and containing incidents (or potential incidents) with the intention of implementing further controls to prevent the recurrence of the event.

2.1.3 Examples of common incidents are listed below:

Type	**Example**
Technical	Hacking Data corruption Infection by malware
Physical	Unescorted visitors in secure areas Break-ins Thefts from secure sites Theft from unsecured vehicles/premises Loss in transit/post
Human	Data input errors Non-secure disposal of hardware, electronic or paper records Unauthorised disclosure of personal information Inappropriate sharing of personal information

2.1.4 The form to report potential data privacy breaches, can be accessed using this link and can also be found in the data protection section of the intranet, must be used to **report ALL suspected data protection breaches.**

2.1.5 B&FC acknowledges that some data breaches and potential breaches are beyond its reasonable control and recognises the importance of being prepared for such eventualities.

2.1.6 B&FC will ensure that it responds appropriately to actual, suspected and potential data breaches occurring via its systems or processes. Structured response will:

- Log the incident ~~log~~, investigate where appropriate and review
- be informed by previous lessons learned and recommendations made
- aim to minimise risk to and deleterious impact on business
- report breach frequency and trends to SMT
- identify and prioritise budgetary and resourcing implications

2.2 Outline Process for incidents

The diagram below shows the expected flow of actions following a personal data breach including a potential personal data breach

2.3 Discover.

Potential and actual breaches, and weaknesses must be reported at the earliest possible opportunity using the using this form that can also be found in the data protection section of the intranet.. Only in urgent circumstances, can incidents be reported in other ways (usually by telephone).

2.4 Assess.

On receiving an automated notification, a member of the Data Protection Team will open incident log and make an assessment of the severity of the breach/potential breach.

2.5 Investigate

The objective of any breach or potential breach investigation is to:

- collect facts to minimise impact of the breach incident to the data subject(s) and the organisation
- determine whether the incident must be reported to the Information Commissioner's Office
- identify whether the data processor (where not B&FC) needs to be notified
- identify actions needed to prevent a recurrence of the incident

Key personnel involved in the potential or actual breach will be interviewed along with their line managers, where applicable, to collect as much relevant information as possible and to quickly determine

- how the breach incident occurred
- what actions have been taken so far
- whether outside agencies are involved or need to be involved
- whether the data subjects have been notified or need to be notified

Once a personal data breach or potential breach has been recorded, the following actions must be carried out by the Data Protection Team as soon as possible:

- Create a folder under Data Breaches using the following format – DPB[Breach Reference Number]
- Save any emails/documents relating to the personal data breach (or potential breach).
- Where the personal data breach or potential breach affects data that B&FC are processing on behalf of someone else, B&FC will notify the data controller without undue delay

2.6 Report.

The purpose of the breach or potential breach report is to:

- document the circumstances of the breach incident
- record any actions taken
- outline recommendations made to the Vice Principal Finance and Planning
- support decisions about whether disciplinary action is appropriate
- support any decision to report breaches to the Information Commissioner's Office

Not all data protection breaches will result in formal action. Some will be false alarms or "near miss" events that do not cause immediate harm to individuals or

the organisation. These should still be reported. Analysis of these will allow lessons to be learnt and facilitate continual improvement.

2.7 Respond.

Pursuant to the UK GDPR, consideration must be given to notifying the affected individual(s) about a significant personal data breach without undue delay.

When assessing whether to notify individuals, B&FC must consider whether the personal data breach is likely to result in a high risk to the rights and freedoms of individuals.

Notifying the individuals is not required under the following circumstances:

- If B&FC as the controller has implemented appropriate technical and organisational protection measures in respect of the personal data affected by the breach, in particular, measures taken which render the personal data unintelligible to persons who are not authorised to access it (for example, encryption)
- If B&FC as the controller has taken measures since the breach which ensure that high risk to the rights and freedoms of the data subjects is no longer likely
- If it would involve disproportionate effort to do so. In such a case, there shall instead be an alternative communication whereby the data subjects are informed in an equally effective manner.

If the DPO considers that a significant breach has occurred, he/she will make a recommendation to the Vice Principal Finance and Planning and the Chief Operating Officer that a formal report should be made to the Information Commissioners Office (ICO). The Vice Principal Finance and Planning and the Chief Operating Officer will respond to the DPO within the required 72 hours deadline as to whether the recommendation will be accepted

If the recommendation has been accepted, the DPO will inform the ICO using the ICO reporting portal and will keep the Vice Principal Finance and Planning and Chief Operating Officer informed of any responses received from the ICO.

The Vice Principal Finance and Planning will inform the Board at the next meeting.

2.8 Review and Improve

Regardless of the type and severity of incident, there are likely to be recommendations to be made even if only to reinforce existing procedures.

There are two categories of recommendation that can be made:

- **Local Recommendations** apply purely to the team(s) affected by the incident. They will usually reflect measures that need to be taken to restrict the chances of a similar incident occurring in the future.
- **Corporate Recommendations** - Some incidents will be caused by factors that are not unique to a single team such as, insufficient training, incorrect information handling, failed physical security. The organisation aims to identify any such risks and put in place measures to prevent similar incidents occurring in the future.

All recommendations will be assigned an owner and a deadline by which they must be implemented. This ensures that

- the organisation responds appropriately to any measures identified
- the response is driven by a single responsible individual
- where incidents are reported to the ICO, B&FC can demonstrate that measures have been put in place or formally agreed. This is an expectation of the ICO.
- where B&FC are the data processor for another organisation, B&FC can demonstrate that measures have been put into place or formally agreed

Key to preventing further incidents is ensuring the organisation learns from an incident. As well as reporting trends to SMT, the DPO will meet regularly with the data protection office team to

- review incidents reported
- hear recommendations
- define and agree actions to be taken
- consider cases which may require escalation or result in disciplinary action

3. Accountability

The Data Protection Officer is accountable to the Corporation for

- monitoring compliance with UK GDPR
- ensuring that B&FC has in place training and procedures to minimise the risk of personal data breaches and potential breaches
- ensuring that personal data breaches and potential breaches and complaints are managed appropriately
- maintaining a register of personal data breaches and potential breaches
- reporting breaches to the Information Commissioner as appropriate
- where B&FC is a data processor, informing the relevant data controller of personal data breaches and potential breaches to the data for which they are responsible

The Head of Management Information & Funding is responsible for supporting the Data Protection Officer in all matters relating to data protection and for coordinating routine operational data protection matters.

The B&FC Executive is responsible for ensuring the Data Protection Officer is supported and resourced to perform this role in an appropriate manner without hindrance.

4. Student Involvement

No direct student involvement.

5. Linked policies

Clean Desk and Clear Screen Policy
Data Privacy Impact Assessment Policy
Data Protection Policy
Information Security Policy

6. Linked procedures

Clean Desk and Clear Screen Procedure
Freedom of Information Code of Practice
Procedure for Data Privacy Impact Assessment
Sharing Information Code of Practice

7. Equality Impact Assessment

Impact Assessment for the 4 strands of Equality, Safeguarding and Inclusion, Health and Safety and Sustainability	
Initial Form to be completed with Risk Assessments or as part of a proposal or change to a policy, plan or new way of working	
Title of Activity: Procedure for Assessing and Reporting Potential Data Breaches Author and Date: Head of MI&F 29 Mar 18	☐ New or ☐ Revision Please tick as appropriate Expected Implementation Date: July 2021 What is the review date? July 2024
Equality, Diversity and Inclusion Which of the characteristics maybe impacted upon? And, if yes, how has this been considered? What are the risks? What are the benefits?	Personal data relating to a range of characteristics, included those protected under the Equality Act, may be deemed sensitive and will be afforded further protection through this procedure
Safeguarding: Are there any aspects of this proposal which could cause a learner/member of staff/visitor to feel unsafe? If yes, how has this been considered? What are the risks? What are the benefits?	☐ Yes ☒ No
Health and Safety: Have any risks been identified? If yes, how has this been considered? What are the risks? What are the benefits?	☐ Yes ☒ No
Sustainability: Are there expected benefits or impacts on sustainability issues? If yes, how have these been considered?	☐ Yes ☒ No
Evidence: What evidence do you have for your conclusions and expectations for these conclusions? How will this impact be monitored for all these considerations?	Procedure is a necessary part of B&FC's data protection framework which contributes towards increased security, safety and protection.
Is this policy of a high/medium or low risk? :	☐ High ☐ Medium ☒ Low