Policy Name:	Data Breach Policy and Procedure
Policy Number/Version No:	Version 2
Effective Date:	March 2021
Review Date:	May 2022
Policy Responsibility:	Data Protection Officer
Approved By:	Audit Committee / Corporation

Introduction

1. The GDPR introduces a duty on the College to report certain personal data breaches to the ICO. This must be done within 72 hours of becoming aware of the breach, where feasible. Richmond Upon Thames College holds, processes, and shares a large amount of personal data, a valuable asset that needs to be suitably protected. Every care is taken to protect personal data from incidents (either accidentally or deliberately) to avoid a data breach that could compromise security. Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative noncompliance, and/or financial costs/ fines. The College is required under GDPR to have in place an institutional framework designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility.

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

Scope

3. This Policy relates to all personal and special category data held by the College regardless of format. This Policy applies to all staff at the College and includes temporary, casual or agency staff and contractors, consultants, suppliers and data processors working for, or on behalf of the College.

4. The objective of this Policy is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches. It also sets out the requirements under GDPR.

Definition / Types of Breach

5. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

6. An incident includes but is not restricted to, the following:

    - Loss or theft 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)
    - Equipment theft or failure
    - Unauthorised use of, access to or modification of data or information systems
    - Attempts (failed or successful) to gain unauthorised access to information or IT system(s)
    - Unauthorised disclosure of personal or special category data
    - Website defacement
    - Hacking attack
    - Unforeseen circumstances such as a fire or flood
    - Human error
    - 'Blagging' offences where information is obtained by deceiving the organisation who holds it

Reporting an incident

7. All individuals who access, use or manage the College's information are responsible for reporting a data breach and information security incidents immediately to the Data Protection Officer (dpo@rutc.ac.uk).

8. If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable. Depending on the level and nature of the breach it may need to be notified out of hours. An Incident Report Form should be completed as part of the reporting process. This is found at annex A to this policy. The report includes 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.

9. When a personal data breach occurs, the College needs to consider whether this poses a risk to people. The likelihood and severity of the risk to people's rights and freedoms, following the breach needs to be considered. When an assessment has been made, if it is likely there will be a risk then the ICO must be notified. If it is unlikely that there is a risk to people's rights and freedoms, then it is not necessary to report the breach to the ICO. It is essential then to report all available facts to the Data Protection Officer without delay so that this assessment is carried out as quickly as possible – considering the obligation to report to the ICO within 72 hours. Not every breach needs to be reported to the ICO.

10. All staff should be aware that any breach of the Data Protection Act may result in the College's Disciplinary Procedures being instigated.

11. The Data Protection Officer (DPO) will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach. An initial assessment will be made by the DPO in liaison with relevant officers to establish the severity of the breach, action to resolve the breach and who will take the lead investigating the breach (this

will depend on the nature of the breach in some cases it could be the DPO). The DPO will determine if it is necessary to report the breach to the Information Commissioner.

12. The DPO will appoint a Lead Investigation Officer (LIO) who will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause. The LIO will establish who may need to be notified as part of the initial containment. Advice from experts across the College may be sought in resolving the incident promptly. The LIO, in liaison with the relevant officer(s) will determine the suitable course of action to be taken to ensure a resolution to the incident.

Investigation and Risk Assessment

13. An investigation will be undertaken by the LIO immediately and wherever possible within 24 hours of the breach being discovered / reported. The LIO will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur. The investigation will need to take into account the following:
    - the type of data involved
    - its sensitivity
    - the protections are in place (e.g. encryptions)
    - what's happened to the data, has it been lost or stolen
    - whether the data could be put to any illegal or inappropriate use
    - who the individuals are, number of individuals involved and the potential effects on those data subject(s)
    - whether there are wider consequences to the breach

Notification

14. Under GDPR, the DPO will need to inform the Data Subject of the breach. If a breach is likely to result in a high risk to the rights and freedoms of individuals, those concerned directly must be notified without undue delay.
    It is a requirement under the Regulations for the breach to be reported to the ICO where it is likely that there is a risk to people's rights and freedoms. The DPO will in certain circumstances take advice from the ICO. It will also be necessary to consider if there are any legal or contractual notification requirements should the breach for example impact on a supplier to the college. The DPO will decide on action to be taken and will be the key point of contact with the ICO.

15. Notification (where appropriate) to the individuals whose personal data has been affected by the incident will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks. Individuals will also be provided with a way in which they can contact the College for further information or to ask questions on what has occurred.

16. The DPO must consider notifying third parties such as the police, insurers, bank or credit card companies, and trade unions. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

17. The DPO will consider whether Marketing should be informed regarding a press release and to be ready to handle any incoming press enquiries. Any press involvement should be approved by the Principal.

18. All actions will be recorded by the DPO.

Evaluation and Response

19. Once the initial incident is contained, the DPO will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken. Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

20. The review will consider:
    - Where and how personal data is held and where and how it is stored
    - Where the biggest risks lie, and will identify any further potential weak points within its existing measures
    - Whether methods of transmission are secure; sharing minimum amount of data necessary
    - Identifying weak points within existing security measures
    - Staff understanding and provision of sufficient training.
    - Implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security

21. If deemed necessary a report recommending any changes to systems, policies and procedures will be considered by the Audit and Risk Committee.

ANNEX A

DATA BREACH REPORT FORM

Please act promptly to report any data breaches or suspected data breaches. If you discover or suspect a data breach, please notify your Curriculum/ Line Manager immediately, complete Section 1 of this form and email it to the Data Protection Officer (DPO) dpo@rutc.ac.uk

Section 1: Notification of Data Security Breach	**To be completed by person reporting incident**
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number):	
Brief description of incident or details of the information lost:	
Number of Data Subjects affected, if known:	
Has any personal data been placed at risk? If, so please provide details:	
Brief description of any action taken at the time of discovery:	

For use by the Data Protection Officer	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	

Section 2: Assessment of Severity	**To be completed by the Lead Investigation Officer / DPO**
Details of the IT systems, equipment, devices, records involved in the security breach:	
Details of information loss:	
What is the nature of the information lost?	
How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT systems?	
Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for the College or third parties?	
How many data subjects are affected?	
Is the data bound by any contractual / legal security arrangements?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories:	
HIGH RISK personal data – **Special Category data** relating to a living, identifiable individual's a) racial or ethnic origin; b) political opinions or religious or philosophical beliefs; c) membership of a trade union; d) physical or mental health or condition or sexual life; e) commission or alleged commission of any offence, f) proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings. g) Sexual orientation h) Genetic or biometric data	
Information that could be used to commit identity fraud such as; personal bank account and other financial information; national identifiers, such as National Insurance Number and copies of passports and visas;	
Personal information relating to vulnerable adults and children;	

Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed;	
Spreadsheets of marks or grades obtained by students, information about individual cases of student discipline or sensitive negotiations which could adversely affect individuals.	
Security information that would compromise the safety of individuals if disclosed.	
Data Protection Officer and/or Lead Investigation Officer to consider whether it should be escalated to the College Leadership Team/ Audit Committee	

Section 3: Action taken	**To be completed by DPO**
Report received by:	
On (date):	
Action taken by responsible officer/s:	
Was incident reported to Police?	**Yes/No** **If YES, notified on (date):**
Follow up action required/recommended:	
Reported to other internal stakeholders (details, dates):	
Notification to ICO	**YES/NO If YES, notified on:** **Details:**
Notification to data subjects	**Date:**
Notification to other external regulator/stakeholder	**YES/NO If YES, notified on:** **Details:**