MERTON COLLEGE DATA PROTECTION BREACH REGULATIONS

1. Approval and binding effect

1.1. These Regulations were approved by the Governing Body of Merton College ("the College") on Wednesday 3 October 2018.

1.2. Any amendments to these Regulations require the Governing Body's approval. The Governing Body approved amendments to this Policy on 19 June 2023.

1.3. These Regulations apply to all personal data held by the College.

1.4. All members of the College and all employees or other staff of the College are bound by these Regulations and **must** comply with them. For the avoidance of doubt any reference to employees or staff shall include permanent, temporary, contract and other support staff as applicable ; and "members" includes both Fellows and Junior Members.

2. Definitions

2.1. "DPO" means the College's Data Protection Officer.

2.2. "GDPR" means the UK General Data Protection Regulation.

2.3. "ICO" means the Information Commissioner's Office.

2.4. 'MUST' and 'SHALL' mean that the item is an absolute requirement.

'MUST NOT' and 'SHALL NOT' mean that the item is absolutely prohibited.

'SHOULD' means that there may exist valid reasons in particular circumstances not to comply with a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

'SHOULD NOT' means that there may exist valid reasons in particular circumstances when particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.

3. Types of breach

Examples of breaches include (but are not limited to):

3.1. Data Breach / Loss/ Theft: physical or digital;

3.2. loss or theft of data or equipment on which data is stored ;

3.3. inappropriate access controls allowing unauthorised use ;

3.4. equipment failure ;
3.5. human error ;

3.6. unforeseen circumstances such as fire or flood ;

3.7. hacking ;

3.8. offences where information is obtained by deception.

4. Reporting a breach or suspected breach

4.1. Any member of the College who discovers, suspects or receives a report of a breach or suspected breach **must** immediately inform the DPO (or, if the DPO is not available, the Finance Bursar ; or, if the Finance Bursar is not available, the Domestic Bursar) and, where the breach involves information technology, the Head of IT.

4.2. Any member of the College's staff who discovers, suspects or receives a report of a breach (or suspected breach) **must** immediately inform the DPO (or, if the DPO is not available, the Finance Bursar ; or, if the Finance Bursar is not available, the Domestic Bursar) and their Head of Department and, where the breach involves information technology, the Head of IT.

4.3. Where under the GDPR the College is under a duty to report a data breach to the ICO, this **must** be done within 72 hours of becoming aware of the breach.[1]

5. Immediate Containment / Recovery

5.1. In a case falling within regulation 4.1:

5.1.1. Where the breach involves information technology, the Head of IT **must** ascertain whether the breach is still occurring ; if so, steps **must** be taken immediately to minimise the effect of the breach;[2]

5.1.2. the DPO and (where the breach involves information technology) the Head of IT **must** ensure that appropriate steps are taken quickly to recover any losses and limit the damage.

5.2. In a case falling within regulation 4.2:

5.2.1. The Head of Department **must** ascertain whether the breach is still occurring. If so, steps **must** be taken immediately to minimise the effect of the breach.[3]

---

[1] The following ICO guidance will help the DPO decide whether and how to notify:

- When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it is likely that there will be a risk then you must notify the ICO; if it is unlikely then you do not have to report it. However, if you decide you do not need to report the breach, you need to be able to justify this decision, so you should document it.
- In assessing risk to rights and freedoms, it is important to focus on the potential negative consequences for individuals. Recital 85 of the GDPR explains that: "A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."
- This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. You need to assess this case by case, looking at all relevant factors.
- If it is decided to report the incident to the ICO, the following link has details on how to do so: https://ico.org.uk/for-organisations/report-a-breach/

[2] E.g. by shutting down a system or alerting relevant staff.

[3] E.g. by shutting down a system or alerting relevant staff.

If the breach involves information technology the Head of Department **should** ask for assistance from IT staff.

5.2.2. The Head of Department **must** check that the the DPO has been informed and **must** also inform the College Officer with supervisory responsibility for the staff concerned as soon as possible.

5.2.3. The DPO and the supervising College Officer, working with the Head of Department, and (where the breach involves information technology) the Head of IT **must** ensure that appropriate steps are taken quickly to recover any losses and limit the damage.

5.3. Steps to recover losses and limit damage might include:

5.3.1. Attempting to recover lost equipment ;

5.3.2. Contacting any affected individuals or departments so that they are prepared for any potentially inappropriate enquiries 'phishing' for further information on those concerned ;

5.3.3. Contacting the relevant people so that they can be prepared to handle any press or other enquiries that may result ;

5.3.4. The use of back-ups to restore lost/damaged/stolen data ;

5.3.5. If bank details have been lost/stolen, contacting banks directly for advice on preventing fraudulent use.

5.4. If the data breach includes any entry codes or passwords, these codes **must** be changed immediately and all relevant employees and members of the College informed.

5.5. The DPO **must** consider whether the police need to be informed. Informing the police 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 given the nature of information lost.

6. Investigation

6.1. The DPO **shall** ensure that the College investigates the breach and ascertains whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation.

6.2. The investigation **should** involve the Head of IT (where the breach involves information technology) and the relevant Head of Department and/or supervising College Officer.

6.3. The investigation **shall** consider: the type of data concerned, its sensitivity, what protections are in place (e.g. encryption), what has happened to the data, whether the data could be put to any illegal or inappropriate use, how many people are affected, what type of people have been affected (the public, suppliers etc.) and whether there are wider consequences to the breach.

6.4. The investigation **shall** be completed urgently and wherever possible within 24 hours of the breach being discovered or reported. A further review of the causes of the breach and recommendations for future improvements **must** be done once the matter has been resolved.

7. Informing and recording

7.1. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the DPO **shall** ensure that the College informs those individuals without undue delay.

7.2. The DPO **shall**, after seeking legal advice (where necessary), decide which agencies and which other persons should be notified of the breach. Some people/agencies may need to be notified as part of the initial containment, but the decision will normally be made once an investigation has taken place.

7.3. The DPO **shall** liaise with the Estates Bursar & Land Agent about informing the College's insurers.

7.4. The DPO **shall** ensure that the College keeps a record of all personal data breaches by reporting them to the Finance Committee (see further paragraph 8.1) and retaining copies of those reports, regardless of whether the College was required to notify data subjects.

8. Evaluation

8.1. In the aftermath of the breach, the DPO **shall** fully review both the causes of the breach and the effectiveness of the response to it and prepare a written report for the next meeting of the Finance Committee.

8.2. If systemic or ongoing problems are identified, an action plan **must** be drawn up and approved by the Finance Committee to correct these.

8.3. If the breach warrants a disciplinary investigation this **shall** be conducted by the appropriate College Officer or Head of Department in accordance with the College's Bylaws and other relevant regulations.

9. Implementation

9.1. All Heads of Department **must** ensure that their staff are aware of these Regulations and their requirements. This should be undertaken as part of induction and supervision.

9.2. The DPO in co-operation with the Finance Bursar, the Sub-Warden, and the Senior Tutor **must** ensure that the Fellows and Junior Members of the College are aware of these Regulations and their requirements.

10. Review and Amendment

These Regulations **shall** be reviewed and updated annually by the Finance Bursar and the DPO and approved by the Governing Body after review by the Finance Committee and the Statutes and Bylaws Committee.

Useful contacts

Data Protection Officer:	dpo@merton.ox.ac.uk
	01865 276310 (College Lodge)
IT Department:	it-support@merton.ox.ac.uk
	01865 276310 (College Lodge)
Head of IT:	head.of.it@merton.ox.ac.uk
	01865 276310 (College Lodge)