| Version Control | | | |
|---|---|---|---|
| Author: | Data Protection Officer | Approved by: | Senior Leadership Team |
| Date Approved: | July 2026 | Next Review Date: | July 2028 |
| Responsible for review: | Senior Leadership Team | Version Number: | 3.0 |
| Version Amendments | | | |
| Date of Amendment: | August 24 (v2) | | |
| Amendments: | Formatting updated to make it easier to read<br>Inclusion of advice on how to receive document in an alternative format<br>Amend text to clarify that criminal record data is not special category data<br>Include text to inform that the ICO must be given a reason if notification of a personal data breach is made outside 72 hours<br>Include text to provide the extent of penalties for not informing the ICO of a personal data breach within 72 hours | | |
| Date of Amendment: | July 26 (V3) | | |
| Amendments: | Formatting updated to make it easier to read | | |

## TABLE OF CONTENTS

1. Overview....3
2. About This Policy....4
3. Scope....5
4. Definitions....5
5. What is a Personal Data Breach....6
6. Reporting a Personal Data Breach....7
7. Managing a Personal Data Breach....7
8. Breach Management Team....8
9. Containment and Recovery....8
10. Assessment of Ongoing Risk....9
11. Notification....9

12. Evaluation and Response.....10

13. Policy Status .....**Error! Bookmark not defined.**

14.....**Error! Bookmark not defined.**

- 12-point font.....**Error! Bookmark not defined.**
- 1.5 spacing .....**Error! Bookmark not defined.**
- Inclusion of advice on how to receive document in an alternative format ..... **Error! Bookmark not defined.**
- Amend text to clarify that criminal record data is not special category data..... **Error! Bookmark not defined.**
- Include text to inform that the ICO must be given a reason if notification of a personal data breach is made outside 72 hours.....**Error! Bookmark not defined.**
- Include text to provide the extent of penalties for not informing the ICO of a personal data breach within 72 hours.....**Error! Bookmark not defined.**

Data Breach Report Form.....12

- Low risk data.....**Error! Bookmark not defined.**
- Medium risk data.....**Error! Bookmark not defined.**
- Sensitive data .....**Error! Bookmark not defined.**
- High risk data.....**Error! Bookmark not defined.**

Data Breach Checklist .....13

- physical safety or emotional wellbeing; .....**Error! Bookmark not defined.**
- reputation/privacy.....**Error! Bookmark not defined.**
- finances; .....**Error! Bookmark not defined.**

- identification (theft/fraud).....**Error! Bookmark not defined.**
- combination of these and other private aspects of their life? .....**Error! Bookmark not defined.**

15.....**Error! Bookmark not defined.**

- Consider most appropriate form of contact considering. the security of the medium as well as the urgency of the situation. .....**Error! Bookmark not defined.**
- 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. **Error! Bookmark not defined.**
- Give specific and clear advice on the steps they can take to protect themselves and what the College can do to help .....**Error! Bookmark not defined.**
- Provide a contact for further information or to ask questions (e.g. a contact name, helpline number or a web page). .....**Error! Bookmark not defined.**
- Consult the ICO guidance .....**Error! Bookmark not defined.**

Personal Data Breach Notification Procedure.....16

- Insurers.....19
- Police.....19
- Employees.....20
- Parents/Guardians.....20
- Sponsors.....20
- Banks.....20
- Contract counterparties.....20


If you require this document in an alternative format, please contact Hequality@tameside.ac.uk

## 1. Overview

Data security breaches are increasingly common occurrences whether caused through human error or via malicious intent. As technology trends change and the creation of data and information grows, there are more emerging ways by which data can be breached. The General Data Protection Regulation, in force since May 2018, requires that personal data breaches are notified within 72 hours. Therefore, it is essential that we have a robust and systematic process to ensure we can respond in a both timely and effective manner.

As an organisation that collects 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. 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.

College Personnel will be signposted to a copy of this Policy when they start and may receive notification of periodic revisions. This Policy does not form part of any College Personnel's contract of employment and the College reserves the right to change this Policy at any time. All College Personnel are obliged to comply with this Policy at all times.

## 2. About This Policy

This Policy explains how the College complies with its obligations to recognise and deal with Personal Data breaches and, where necessary, to notify the Information Commissioner's Office (ICO) and the affected individuals.

The aim of this policy is to provide rules and procedures for the notification of personal data breaches across the College to ensure that:

- Data breach events are identified, categorised, reported, investigated and monitored consistently.
- Incidents are assessed and responded to appropriately.
- Appropriate breaches are reported to the supervisory authority (ICO) in a timely manner.
- External bodies or data subjects are informed as required.
- Action is taken to reduce the impact of disclosure.
- Incidents are dealt with in a timely manner and normal operations restored.

- improvements are made and put in place to prevent recurrence where possible.
- All incidents are recorded and documented, whether reportable or not.

The College has a corresponding Personal Data Breach Notification Procedure and Personal Data Breach Register that set out how the College deals with and records Personal Data breaches.

## 3. Scope

This Policy applies to all College Personnel who collect and/or use Personal Data relating to individuals.

It applies to all Personal Data stored electronically, in paper form, or otherwise.

## 4. Definitions

4.1 **College** – Tameside College.

4.2 **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 work on behalf of the College.

4.3 **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.

4.4 **Data Protection Officer** – The Data Protection Officer is Dave Dobson and can be contacted at: DPO@tameside.ac.uk. The DPO may delegate responsibility for specific tasks to other members of College management.

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

4.6 **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.

4.7 **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, and sexual life or sexual orientation.

## 5. What is a Personal Data Breach

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.

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.

A Personal Data breach could include any of the following:

- loss or theft of Personal Data or equipment that stores Personal Data;
- 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 ransomware 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.

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

College Personnel must immediately notify any Personal Data breach to the Data Protection Officer, 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.

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

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

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

- cause, containment and recovery;
- assessment of on-going risk;
- notification;
- evaluation and response.

Each of these four elements will need to be actioned in accordance with the Data Breach Checklist (Appendix 2). An activity log for recording the timeline of the incident management should also be completed (Appendix 3).

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

## 8. Breach Management Team

The Breach Management Team consists of senior managers led by and in support of the Data Protection Officer (DPO).

- Vice Principal Finance and Infrastructure / Data Protection Officer
- Head of HR
- Head of IT
- Director of MIS & IT

Duties stated as being carried out by the Data Protection Officer may be delegated to this group, a member of this group or another College manager where appropriate.

Additional internal staff will be brought in to provide support, advice and expertise depending on the nature and severity of the personal data breach.

The team will meet following receipt of information regarding a breach. Where any member of the team is absent a deputy may be called if appropriate.

Scheduled meetings will also take place termly to discuss wider issues, suggested procedure or document changes, training issues and to review and report on recent activity. Termly reports will be presented to SLT and shared with Governors under 'Risk'.

## 9. Containment and Recovery

An initial assessment of the Personal Data breach will be carried out by the Data Protection Officer.

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.

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:

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

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.

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

## 10. Assessment of Ongoing Risk

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 College 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.

## 11. Notification

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

Any notification will be made by the Data Protection Officer following the College's Data Breach Notification Procedure. The notification shall comply with the requirements of the ICO.

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 College in accordance with the Data Breach Notification Procedure immediately. The ICO must be given a reason if notification of a Personal Data breach takes more than 72 hours.

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.

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.

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.

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. Subsequent notifications to the ICO must be made as soon as possible. Any delay in notifying the ICO must be seen as exceptional and shall be authorised in accordance with the Data Breach Notification Procedure. The ICO must be given a reason if notification of a Personal Data breach takes more than 72 hours. Failing to notify the ICO of a breach when required to do so can result in a heavy fine of up to £8.7 million or 2 per cent of global turnover. The fine can be combined with the ICO's other corrective powers.

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.

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.

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.

## 12. Evaluation and Response

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.

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.

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.

## Appendix 1: Data Breach Report Form

Wherever possible, a data breach should be reported using the Microsoft Form on the Data Protection SharePoint site available via this link to data breach form. Where this is not possible, the below can be used

| | |
|---|---|
| Description of the Data Breach: | |
| Time and date breach was identified and by whom: | |
| Name of person reporting data breach (Include Name, Dept and Tel Extn): | |
| Classification of data breached:<br>• Low risk data<br>• Medium risk data<br>• Sensitive Data<br>• High risk data | |
| Volume of data involved: | |
| Confirmed or suspected breach? | |
| Is the breach contained or ongoing? | |
| If ongoing what containment actions are being taken? | |
| Who has been informed of the breach? | |
| Any other relevant information: | |

This form must be emailed to DPO@tameside.ac.uk. Ring 0161 908-6682 to let Dave Dobson know that the form is being sent

| | |
|---|---|
| Received by: | |
| Date/Time: | |

**Appendix 2: Data Breach Checklist**

Description: _____ Date:_____

| **A** | **Cause, Containment & Recovery** | **What was the main cause and what can be done immediately to mitigate the loss and/or impact** | |
|---|---|---|---|
| **Step** | **Action** | **Guidance Notes** | **Comments relating to this specific breach** |
| A1 | Identify the cause of the breach and whether the breach has been contained<br><br>Ensure any possibility of 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 relevant departments who may be able to assist in this process.*<br><br>*This may involve actions such as taking systems offline or restricting access to systems to a very small number of staff until more is known about the incident.* | |
| A2 | Determine whether anything can be done to recover any losses and/or limit any damage that may be caused | *E.g. physical recovery of data/equipment, or where data corrupted, through use of back-ups*. | |
| **B** | **Risk Assessment** | **Identify and assess any on-going risks and breach severity** | |
| **Step** | **Action** | **Guidance Notes** | **Comments relating to this specific breach** |
| B1 | What type and volume of data is involved? | *Identify what data was involved. List fields where appropriate and record breach severity.* | |
| B2 | If the data was lost/stolen, what safeguards are in place to prevent access/misuse? | *E.g. encryption of data/device.* | |
| **C** | **Notification** | **Who do we need to notify, how and when?** | |
| **Step** | **Action** | **Guidance Notes** | **Comments relating to this specific breach** |
| C1 | Is the breach considered to be reportable under GDPR? | | |

| | | | |
|---|---|---|---|
| C2 | In addition to the rules of GDPR/ Data Protection are there any other legal, contractual or regulatory requirements to notify? | *E.g. terms of funding; contractual obligations* | |
| C3 | Does the College require legal advice? | | |
| C4 | 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, funders, trade unions, website/system owners, bank/credit card companies.* | |
| C5 | How can we notify individuals and what information should we be providing? | • *Consider most appropriate form of contact considering. the security of the medium as well as the urgency of the situation.*<br>• *Provide a contact for further information or to ask questions (e.g. a contact name, helpline number or a web page).*<br>• *Consult the ICO guidance*<br>• *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.*<br>• *Give specific and clear advice on the steps they can take to protect themselves and what the College can do to help* | |
| C6 | Are there wider consequences to consider? | *E.g. likely media coverage, loss of public confidence* | |

| **D** | **Evaluation of Response** | **To evaluate the effectiveness of the response to the breach.** | |
|---|---|---|---|
| **Step** | **Action** | **Guidance Notes** | **Comments relating to this specific** |
| D1 | Identify responsibility for breach, where appropriate, and any interventions that could have prevented this breach. | *This may be an external company, internal or external individuals or natural disaster.*<br>*Where a company or individual was at fault, how is this being addressed and what interventions could have been implemented which would have prevented this breach or provided prior warning.* | |
| D2 | Consider any actions that can be taken to ensure such a breach is prevented or mitigated in the future | *This may include additional safeguards, updates, training or other. Where a policy amendment is needed this should be made, agreed and communicated quickly.* | |
| D3 | Report on findings and implement recommendations. | *The Breach Management Team should provide a full report to SMT following all data breaches, whether reportable to the ICO or not.* | |

## Appendix 3: Personal Data Breach Notification Procedure

Where there is a data breach within the College, it is a legal requirement to notify the ICO within 72 hours and the individuals concerned as soon as possible in certain situations. It is essential therefore that all data breaches, no matter how big or small, are reported to us.

This Procedure should be read in conjunction with our Personal Data Breach Policy and Data Protection Policy. Our Personal Data Breach Policy contains detailed information on what constitutes a data breach; please read it to make sure that you aware of the breadth of the concept of a data breach.

This procedure should be followed by all staff. At all stages of this procedure, our Data Protection Officer and management will decide whether to seek legal advice. This procedure will also apply where we are notified by any third parties that process personal data on our behalf that they have had a data breach which affects our personal data.

The procedure is set out below. Any failure to follow this procedure may result in disciplinary action.

| Identifying and Reporting a Data Breach |
| --- |
| If you discover a data breach, however big or small, you must report this to our Data Protection Officer immediately. The Data Protection Officer is **Dave Dobson** and can be contacted at: 0161 908 6682 or DPO@tameside.ac.uk. Where possible you should complete and send the Data Breach Report Form.<br><br>Any other questions about the operation of this procedure or any concerns that the procedure has not been followed should be referred in the first instance to the Data Protection Officer.<br><br>A data breach could be as simple as you putting a letter in the wrong envelope and therefore even the most minor data breaches ***must*** be reported.<br><br>False alarms or even breaches that do not cause any harm to individuals or to the College should nevertheless be reported as it will enable us to learn lessons in how we respond and the remedial action we put in place.<br><br>We have a legal obligation to keep a register of all data breaches, no matter how big or small and no matter whether any harm was caused. Please ensure that you do report any breach, even if you are unsure whether or not it is a breach. |

APPENDIX 3

## Becoming Aware of a Data Breach - Investigating

We become aware of a data breach when we have a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised. From this point, our time limit for notification to the ICO will commence.

When you report a data breach to our Data Protection Officer, our Data Breach Management Team will promptly investigate the breach to determine whether a breach has occurred that has led to personal data being compromised.

This will be done within 24 hours of a breach being reported to us.

## Assessing a Data Breach

Once you have reported a breach and our Breach Management Team has investigated it and has determined that a breach has occurred, our Data Protection Officer will log the breach in the Data Breach Register and will carry out an initial assessment of the breach to evaluate its severity. The Data Breach Checklist may be used to document the investigation.

Once the level of severity is known, our Data Protection Officer will notify management. If necessary, the Data Breach Team will appoint a response team which may involve for example our HR and IT teams and we will assign responsibility for particular tasks as necessary across the response team.

We will then investigate the breach and consider any on-going risks to the College and any individuals affected.

APPENDIX 3

If our Data Protection Officer and Breach Management Team consider that the breach is very serious, they will consider the impact on our reputation and the effect it may have on the trust placed in us. Our Data Protection Officer and senior management will consider whether to appoint a PR professional to advise on reputational damage and will also consider whether legal advice is needed.

This will be done within 24 hours of us becoming aware of the breach.

## Formulating a Recovery Plan

Our Data Protection Officer and Breach Management Team will investigate the breach and consider a recovery plan to minimise the risk to individuals. As part of the recovery plan, we may enlist the assistance of internal and external experts and also interview any key individuals involved in the breach to determine how the breach occurred and what actions have been taken.

This will be done within 24 hours of assessing the breach.

## Notifying a Data Breach to the ICO

Unless the breach is unlikely to result in a risk to the rights and freedoms of individuals, we must notify the breach to the ICO within **72 hours** of becoming aware of the breach. We must also notify the individuals concerned as soon as possible where the breach is likely to result in a high risk to their rights and freedoms.

The content of the notification will be drafted by our Data Protection Officer in line with our Personal Data Breach Policy, and the notification will be made by our Data Protection Officer – please be aware that **under no circumstances must you try and deal with a data breach yourself**.

This will be done within 72 hours of becoming aware of the breach.

## Notifying a Data Breach to Individuals

We must also notify the individuals concerned as soon as possible where the breach is likely to result in a high risk to their rights and freedoms.

The content of the notification will be drafted by our Data Protection Officer in line with our Personal Data Breach Policy and in conjunction with consulting the ICO if considered necessary. We will notify individuals in clear and plain language and in a transparent manner (for example by email, SMS or letter). Please be aware that **under no circumstances must you try and deal with a data breach yourself.**

In some circumstances, explained in our Personal Data Breach Policy, we may not need to notify the affect individuals. Our Data Protection Officer will decide whether this is the case.

This will be done as soon as possible after we become aware of the breach.

## Notifying a Data Breach to Other Relevant Third Parties

We may also consider that it is necessary to notify other third parties about the data breach depending on the nature of the breach. This could include:

- Insurers
- Police

- Employees
- Parents/Guardians
- Sponsors
- Banks
- Contract counterparties

The decision as to whether any third parties need to be notified will be made by our Data Protection Officer and management. They will decide on the content of such notifications.

This will be done within 5 working days of becoming aware of a data breach.

## Consider Whether Notifications Need to be Updated

We need to keep the ICO up to date about the data breach. If anything changes from the time we send the initial notification to the ICO, our Data Protection Officer will consider whether we need to update the ICO about the data breach.

This will be considered on an ongoing basis.

## Evaluation and Response

The key to preventing further incidents is to ensure that the College learns from previous incidents.

It is extremely important to identify the actions that the College needs to take to prevent a recurrence of the incident. Our Data Protection Officer and management will carry out an evaluation as to the effectiveness of our response to the data breach and document this in our Data Breach Register.