CITY OF WOLVERHAMPTON COLLEGE

Data Breach

Policy and Procedure 2026-27

GDPR Manager

Publication: August 2026

Review: August 2027 Version No. 1

1. Policy Statement

1.1. City of Wolverhampton College is committed to meeting its obligations under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and all applicable regulatory requirements. We maintain a robust, structured, and continuously monitored compliance framework to ensure that personal data is processed securely, lawfully, and transparently.

1.2. As part of our commitment to data protection, we conduct regular risk assessments and gap analyses to evaluate the effectiveness of our policies, procedures, and controls. These reviews enable us to identify areas for improvement and ensure that appropriate mitigating actions are implemented where necessary.

1.3. While we strive to minimise risks through strong governance and technical safeguards, we recognise that data breaches may still occur. This policy outlines our approach to identifying, reporting, managing, and mitigating personal data breaches in a timely and effective manner.

1.4. In the event of a data breach, the College has established clear procedures to:

- Detect and report breaches promptly
- Assess the risk to individuals and the organisation
- Contain and investigate incidents
- Notify the Information Commissioner's Office (ICO) and affected individuals where required
- Implement corrective actions to prevent recurrence

1.5. All data breaches, regardless of severity, will be handled in accordance with GDPR requirements and current data protection legislation. Staff are expected to be aware of their responsibilities and to report any suspected or actual data breaches immediately, in line with college procedures.

1.6. Through this policy, City of Wolverhampton College demonstrates its commitment to maintaining high standards of data protection, ensuring accountability, and protecting the rights and freedoms of all individuals whose data we process.

2. Purpose

2.1. The purpose of this policy is to set out the College's intent, objectives and procedures regarding data breaches involving personal information.

2.2. In line with our obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, the college is required to implement and maintain appropriate procedures, controls, and measures to safeguard personal data. These arrangements are communicated to all employees to ensure they understand their responsibilities, as well as the protocols and reporting lines for identifying and reporting data breaches.

2.3. This policy outlines the College's approach to the timely reporting, communication, management, and investigation of data breaches and related incidents, ensuring compliance with legal and regulatory requirements and the protection of individuals' rights and freedoms.

3. Scope

3.1. This policy applies to all individuals working for or on behalf of City of Wolverhampton College, including permanent, fixed-term and temporary staff, agency workers, volunteers, interns, contractors, third-party representatives, sub-contractors, and agents engaged by the College.

3.2. Compliance with this policy is mandatory. Failure to adhere to its requirements may result in disciplinary action, and where appropriate, contractual or legal consequences.

3.3. In the event of a personal data breach or suspected breach, staff must act immediately in accordance with the College's Data Breach Procedure. *Further guidance on immediate actions can be found in the* Staff Guidelines *section (see page 9)*

4. Data Security & Breach Requirements

4.1. City of Wolverhampton College defines a personal data breach as any security incident that results in the destruction, loss, alteration, unauthorised disclosure of, or access to personal data, whether due to system failure, human error, or inadequate controls.

4.2. The College adopts a *"Privacy by Design and Default"* approach and is committed to ensuring personal data is protected at all stages of processing. Our technical and organisational measures are detailed within the Data Protection and Information Security policies. We undertake regular information audits and risk assessments to identify, classify, and protect personal data, ensuring that appropriate safeguards are in place based on risk.

4.3. Key security measures include:

- Mandatory data protection and IT security training for staff
- Clear desk and screen-lock practices
- Network monitoring, filtering, and anti-malware protection
- Controlled physical access to buildings and secure storage of records
- Secure disposal of information in line with retention schedules
- Encryption of electronic personal data
- Access controls based on a "need-to-know" basis
- Regular review of system security, resilience, and data availability
- Business Continuity and Disaster Recovery arrangements
- Oversight of data sharing, transfers, and disposal processes

These measures ensure the confidentiality, integrity, and availability of personal data and support the College in preventing, detecting, and responding to data breaches effectively.

5. Objectives

- To comply with UK GDPR and the Data Protection Act 2018, ensuring robust procedures and controls for identifying, reporting, investigating, and recording personal data breaches
- To implement and maintain appropriate technical and organisational measures to safeguard personal data and ensure a high level of security
- To use information audits and risk assessments to map data processing activities and minimise the risk of breaches
- To maintain effective risk management processes for assessing and mitigating risks associated with personal data processing
- To ensure all personal data breaches are reported and managed in line with regulatory requirements, including notification to relevant authorities where applicable
- To ensure that notifiable breaches are reported to the Information Commissioner's Office (ICO) without undue delay and, where required, within 72 hours of becoming aware of the breach
- To record all data breaches using the College's Data Breach Incident Form, regardless of severity, to identify trends and improve controls
- To investigate breaches thoroughly, identify root causes, and implement corrective actions to prevent recurrence
- To ensure the Data Protection Officer (DPO) is informed of and involved in all data breach incidents and associated risk assessments
- To protect the rights, freedoms, and personal data of students, staff, and other individuals whose information is processed by the College

6. Data Breach Procedures & Guidelines

6.1. The College has established robust objectives and controls to prevent personal data breaches and to manage them effectively should they occur. Procedures and guidelines for the identification, investigation, and notification of breaches are outlined within this policy.

6.2. This Data Breach Policy is designed to minimise the impact of any incidents and to ensure that all required notifications are made in accordance with legal and regulatory obligations. Staff must refer to the *Staff Guidelines* section (see page 9) for instructions on immediate actions in the event of a breach

7. Breach Monitoring & Reporting

7.1. The College has appointed a Data Protection Officer (DPO) who is responsible for overseeing the investigation of all personal data breaches, regardless of their severity, impact, or level of containment. All breaches must be reported to the DPO without delay and will be managed in accordance with the procedures outlined in this policy.

7.2. All data breaches are subject to investigation, including those that do not meet the threshold for external notification. A comprehensive record of all incidents is maintained to support trend analysis, risk assessment, and continuous improvement of controls.

7.3. Where a data breach is identified as resulting from a system or process failure, appropriate remedial actions will be implemented. Any changes to processes or controls will be formally documented in line with the College's Change Management and Document Control procedures

8. Breach Incident Procedures

8.1. Identification of an Incident

As soon as a data breach has been identified, it is reported to the direct line manager and the Data Protection Officer immediately so that breach procedures can be initiated and followed without delay. Staff should refer to the *Staff Guidelines* (see page 9) for further instruction.

8.2. Prompt and accurate reporting of incidents is essential to ensure compliance with legal and regulatory requirements. The purpose of reporting is to enable effective management of the breach and is not intended to apportion blame. These procedures are in place to protect the College, its staff, students, and all third parties whose data may be affected.

8.3. Upon notification of a breach, immediate steps must be taken to contain the incident and limit any potential impact. While specific containment actions will vary depending on the nature of the breach, the objective is to prevent further unauthorised access, disclosure, loss, or damage to personal data.

All actions taken to contain the breach must be fully documented within the Data Breach Incident Form.

9. Breach Recording

9.1. The College uses a Data Breach Incident Form to record all personal data breaches, regardless of severity or outcome. Completed forms are securely stored (electronically or in hard copy) and reviewed periodically to identify trends, recurring issues, and opportunities for improvement.

9.2. The Data Protection Officer (DPO) is responsible for overseeing the investigation of all breaches, coordinating appropriate containment actions, ensuring accurate documentation, and determining whether notification to the Information Commissioner's Office (ICO) and/or affected individuals is required.

9.3. The Breach Incident Form must be completed as soon as practicable following containment of the breach. A full investigation will be undertaken, with findings, risk assessment, and remedial actions recorded. Outcomes will be communicated to relevant staff and senior management, and records retained for audit and compliance

purposes.

9.4. Where required, breaches will be reported to the ICO without undue delay and, where feasible, within 72 hours of awareness, in line with UK GDPR requirements. Affected individuals will also be informed where there is a high risk to their rights and freedoms.

9.5. All external notifications will be made using the ICO's prescribed reporting channels. Individuals affected by a breach will be provided with clear information about the incident, its potential impact, and any actions taken to mitigate risks.

10. Breach Risk Assessment

10.1. Human Error

Where a personal data breach is identified as resulting from human error, a root cause analysis will be conducted and a formal meeting held with the employee(s) involved.

Relevant procedures and controls associated with the breach will be reviewed, and a risk assessment completed in accordance with the College's Risk Assessment Procedures. Any identified gaps or weaknesses that contributed to the breach will be addressed, with appropriate corrective actions implemented to reduce the likelihood of recurrence.

Outcomes for employees following an investigation may include, but are not limited to:

- Targeted retraining in data protection and compliance requirements
- Reassessment of data protection knowledge and understanding
- Temporary or permanent removal from duties involving personal data processing
- Formal action in line with the College's Disciplinary Procedures

11. System Error

11.1. Where a personal data breach is identified as resulting from a system error, technical failure, or cybersecurity incident, the ICT team will work in conjunction with the Data Protection Officer (DPO) to investigate the incident, assess the associated risks, and determine the root cause.

11.2. A review of the affected systems, controls, and processes will be undertaken, including a gap analysis where appropriate. Findings, actions taken, and recommendations for improvement will be documented within the Data Breach Incident Form. Any weaknesses or control failures identified as contributing to the breach will be addressed through appropriate corrective actions and risk mitigation measures to reduce the likelihood of recurrence.

11.3. Depending on the nature of the incident, actions to contain and mitigate the impact may include, but are not limited to:

- Recovering lost, stolen, or compromised equipment and information where possible
- Isolating, restricting, or shutting down affected systems or services
- Suspending or restricting user access where necessary to prevent further risk

- Restoring data from secure backups where information has been lost, damaged, or corrupted
- Securing physical premises or locations affected by the incident
- Resetting passwords, access credentials, encryption keys, or entry codes where security has been compromised
- Applying security patches, software updates, or configuration changes to address vulnerabilities
- Increasing system monitoring to identify any ongoing or further risks
- All containment and remediation actions must be recorded as part of the breach investigation process and reviewed to ensure their effectiveness.

12. Assessment of Risk and Investigation

12.1. Following the identification and containment of a personal data breach, the Data Protection Officer (DPO) will assess the nature and extent of the incident to determine the level of risk to affected individuals and any actions required to mitigate further harm.

12.2. The investigation should consider:

- The type and volume of personal data involved
- Whether special category data or other sensitive information is affected
- The number of individuals impacted
- The security measures in place at the time of the breach (e.g. encryption, access controls, pseudonymisation)
- The cause and circumstances of the breach
- The location and status of the information, including whether it has been accessed, disclosed, lost, altered, or recovered
- The potential impact on affected individuals, including risks to their rights and freedoms
- Any wider organisational, legal, regulatory, financial, or reputational implications.

12.3. A lead investigator will be appointed where appropriate and will maintain a detailed record of the investigation. This record should include:

- A description of the incident and how it occurred
- Actions taken to contain and mitigate the breach
- Evidence gathered during the investigation
- Notes of meetings, interviews, and relevant communications
- The risk assessment and investigation findings
- Decisions relating to ICO and data subject notifications
- Corrective actions, lessons learned, and recommendations for improvement.

12.4. A final investigation report will be completed and retained in accordance with the College's record management and data protection requirements. Any identified

improvements to policies, procedures, systems, or training will be implemented to reduce the risk of similar incidents occurring in the future.

13. Breach Notifications

13.1. The College recognises its legal obligation to report certain personal data breaches in accordance with the UK GDPR, the Data Protection Act 2018, and the Data (Use and Access) Act 2025.

13.2. All staff must report actual or suspected personal data breaches immediately through the College's established reporting channels to ensure that incidents are identified, assessed, and escalated without undue delay.

13.3. The Data Protection Officer (DPO) will assess each breach to determine whether notification to the Information Commissioner's Office (ICO) and/or affected individuals is required.

14. Information Commissioners Office Notification

14.1. The ICO must be notified where a personal data breach is likely to result in a risk to the rights and freedoms of individuals.

14.2. Where notification is required, the College will report the breach to the ICO without undue delay and, where feasible, within 72 hours of becoming aware of the breach. If notification is not made within 72 hours, the reasons for the delay will be documented and provided to the ICO.

14.3. In accordance with Article 33 UK GDPR, the College may determine that notification is not required where the breach is unlikely to result in a risk to the rights and freedoms of individuals.
Where required, notifications to the ICO will include:

- A description of the nature of the personal data breach
- The categories and approximate number of individuals affected
- The categories and approximate number of personal data records concerned
- The name and contact details of the Data Protection Officer or other relevant contact point
- A description of the likely consequences of the breach
- Details of measures taken, or proposed, to address the breach and mitigate any adverse effects

All personal data breaches will be recorded and investigated regardless of whether notification to the ICO is required.

14.4. Where the College acts as a data processor on behalf of another organisation, the relevant data controller will be informed without undue delay upon becoming aware of a personal data breach. Where the College engages third-party processors, contractual arrangements will require those processors to notify the College without undue delay of any actual or suspected personal data breach affecting College data.

15. Data Subject Notification

15.1. When a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, The college will always communicate the personal data breach to the data subject without undue delay, in a written, clear and legible format.

15.2. Where a personal data breach is likely to result in a high risk to the rights and freedoms of individuals, the College will notify affected individuals without undue delay.

Notifications will be provided in clear and plain language and will include:

- The nature of the personal data breach
- The contact details of the Data Protection Officer or another appropriate contact point
- The likely consequences of the breach
- The measures taken, or proposed to be taken, to address the breach and mitigate any adverse effects.

15.3. The College may not be required to notify data subjects where:

- Appropriate technical and organisational measures, such as encryption, rendered the data unintelligible to unauthorised persons;
- Subsequent measures have ensured that a high risk to individuals is no longer likely to materialise; or
- Individual notification would involve disproportionate effort, in which case a public communication or similar measure may be used.

16. Record Keeping

16.1. The College will maintain a record of all personal data breaches, regardless of whether they require notification to the ICO or affected individuals.
Records will include:

- The facts relating to the breach
- The effects and potential impact of the breach
- Investigation findings
- Decisions regarding notifications
- Corrective and preventative actions taken

16.2. All breach records will be authorised by the Data Protection Officer and retained in accordance with the College's Records Retention Schedule for a minimum period of six years from the closure of the incident.

17. Responsibilities

17.1. The College will ensure that all staff are provided with the time, resources and support to learn, understand and implement all procedures within this document, as well as understanding their responsibilities and the breach incident reporting lines.

17.2. The Data Protection Officer is responsible for regular compliance audits and

gap analysis monitoring and the subsequent reviews and action follow ups. There is a continuous audit trail of all compliance reviews and procedural amendments and feedback to ensure continuity through each process and task. Managers are responsible for ensuring staff are aware of reporting requirements, escalating breaches promptly and supporting investigations and containment activities.

17.3. All staff are responsible for protecting personal data in accordance with college policies, reporting actual or suspected breaches immediately and cooperating with investigations and corrective actions.

18. Breach Incident Procedures – Staff Guidelines

18.1. Identification of an Incident

- As soon as a data breach has been identified, it is reported to the direct line manager and the Data Protection Officer immediately so that breach procedures can be initiated and followed without delay.
- Cooperate fully with any investigation and reporting incidents in full and with immediate effect is essential to the compliant processing of the College.
- Some personal data breaches may require notification to the ICO within 72 hours of the College becoming aware of the incident.
- Prompt reporting is essential to protect affected individuals, support compliance with data protection legislation, and minimise harm

19. Breach Recording

- The College utilises a Data-Breach-Incident-Form.docx
- for all incidents, which is completed for any data breach, regardless of severity or outcome.
- Staff may be require completing the Breach Incident Form in some cases staff reporting a breach may be asked to provide the following information:
- Date and time the breach occurred (if known)
- Date and time the breach was identified
- Description of the incident
- Type of personal data involved
- Approximate number of individuals affected
- Actions taken to contain the breach
- Equipment, systems, or locations involved
- Individuals notified
- Potential risks or impacts identified

All breach records will be retained for compliance, audit, and continuous improvement purposes.