Data Protection Impact Assessment (DPIA)

Policy and Procedure 2026-27

GDPR Manager

Publication Date: August 2026

Review Date: August 2027 | Version No. 1.0

1. Policy Statement

1.1. The City of Wolverhampton College is committed to protecting the rights and freedoms of individuals whose personal data we process. This Data Protection Impact Assessment (DPIA) Policy outlines our approach to identifying, assessing, and mitigating data protection risks in line with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

1.2. DPIAs are a key part of the College's accountability obligations and support lawful, fair, and transparent processing of personal data.

2. Purpose

2.1. The Policy explains how City of Wolverhampton College Identifies, conducts, documents and reviews Data Protection Impact Assessments (DPIAs) to ensure data protection by design and by default, and to demonstrate accountability. To also Identify and reduce privacy risks for students, staff, applicants, apprentices, contractors, and other individuals. To establish a consistent framework for completing DPIAs throughout the college. DPIAs are Required under UK GDPR Article 35 when processing is likely to present a high risk to individuals' and freedoms. If any high risk remains unmitigated, the college must consult the ICO before processing, as required by Article 36.

3. Scope

3.1. This Policy applies to:

- All college staff, governors, contractors, third parties and processors acting on the College's behalf.
- All new or significantly modified processing activities, projects, vendors, research and operational processes involving personal data, including data related to students, staff, alumni, applicants, visitors, and placement partners.
- All personal data, including special category and criminal offence data, this includes but not limited to:
    - Student and applicant data.
    - Staff and governor data
    - Apprenticeship and wellbeing information
    - Safeguarding and wellbeing information.
    - CCTV, biometrics, and monitoring systems
    - Learning technologies and digital platforms
- All processing under UK GDPR and the Data Protection Act 2018.

4. Definition

4.1. Data protection Impact Assessment (DPIA): - A DPIA is a process designed to help you systematically analyse, identify and minimise the data protection risks of a project or plan. It is a key part of your accountability obligations under the UK GDPR, and

when done properly helps you assess and demonstrate how you comply with all your data protection obligations.

4.2. High risk: - This can be defined as a risk with either high likelihood of harm, or a lower likelihood of serious harm (including physical, material or non-material harm)

4.3. Residual risk: - This can be defined as the risk remaining after all reasonable mitigations, if still high, prior consultation with the ICO is required (Art. 36).

5. Legal Framework

- This policy is informed by:
  - UK General Data Protection Regulation (UK GDPR)
  - Data Protection Act 2018
  - ICO Guidance on Data Protection Impact Assessments.

6. When a DPIA is Required

6.1. A DPIA must be completed where processing is likely to result in a high risk to individuals' right and freedoms, including where the college undertakes:

- Large-scale processing of special category data (e.g. health, safeguarding, disability support).
- Systematic monitoring of individuals (e.g. CCTV, online learning monitoring tools).
- Use of new or innovative technologies (e.g. AI-based learning analytics), Automated decision-making that has legal or significant effects.
- Data sharing with external partners or agencies in new ways.
- Processing involving children or vulnerable individuals.

6.2. Good practice: The College will also conduct DPIAs for other major Projects involving personal data to support Privacy by design and accountability, a DPIA should also be considered where there is any uncertainty about risk

7. Roles and Responsibilities

7.1. Governing Body: - Provides oversight and assurance that DPIAs are embedded in college governance.

7.2. Principal and Senior Leadership Team: - Ensure resources and support for effective DPIA completion, reviews escalated DPIAs with residual high risk and, Promote a culture of data protection compliance.

7.3. Data Protection Officer (DPO): - Advise on whether a DPIA is required, necessity, scope, methodology and mitigations.

7.4. Reviews and provides feedback on DPIAs, monitoring compliance and acting as point of contact with ICO/ leads ICO prior consultation where required. (Article 39)

7.5. Project Leads/Information Asset Owners (IOA): -Identify processing activities that require DPIA and ensure a DPIA is initiated early, completed accurately, and mitigations are implemented and evidenced.

7.6. Project Manager/Product Owner: - Coordinates the DPIA activities; maintains the action log; ensures suppliers cooperate.

7.7. Procurement & IT Security: - Ensures DPIA completion is a gate in procurement/change; provides security due diligence, technical controls and assurance.

7.8. Third- party Processors: - Must provide sufficient information/security assurances to support the college's DPIA and comply with college instructions.

7.9. All Staff: - comply with this policy and consult with the DPO when proposing new uses of good practise

8. DPIA Triggers and Screening

8.1. Screening: For every new project/change involving personal data, the Project Manager completes **The DPIA Screening Questionnaire** in the college template. If any high-risk indicators are flagged, proceed to full DPIA.

8.2. Typical College use-cases that usually require a DPIA: - New or changed learning platforms, proctoring/monitoring tools, or AI-enhanced analytics about students/staff.

8.3. CCTV expansions. ANPR on premises, monitoring tools affecting behaviours.

8.4. Large-scale processing of special category data (e.g. learner support/health, safeguarding, EDI).

8.5. Data sharing with partners/employers for placements, or new cloud mitigation/Saas vendors.

9. DPIA Process

9.1. Step 1 – Initiate early: Start at concept or at the initial stage of the project.

9.2. Step 2 – Describe processing: Nature, scope, context, purposes; data categories; data subjects; data flows; recipient.

9.3. Step 3 – Assess necessity & proportionality: Why personal data are needed, alternatives, data minimisation, privacy notices, rights enablement, DPIA alignment with principles.

9.4. Step 4 – Risk assessment: Identify risks to individuals (likelihood/severity), including discrimination, identity theft, financial loss, distress, reputational harm, or minor effects on rights.

9.5. Step 5 – Mitigations & controls: Technical /organisational measures (security, access, encryption, pseudonymisation, logging/monitoring, supplier controls, training). Record residual risk after control.

9.6. Step 6: Consult: DPO (mandatory), and where appropriate, data subjects or representatives, unions, student unions, subject – matter experts; processors must assist.

9.7. Step 7: Sign-off & integrate: The GDPR manager advice recorded; Sponsor/IAO (information asset Owner) accepts risk and commits to actions; embed outcomes into project plan, contract, and change controls.

9.8. Step 8: Prior consultation (if needed): if residual risk remains high, the GDPR Manager leads consultation with the ICO before processing begins, providing all required details; processing must not start until ICO advice received. The ICO normally replies within 8 weeks (extendable to 14 in complex cases).

9.9. Step 9: Review & update: Treat the DPIA as a living document; review at least annually and at each major change; re-assess risks after incidents or new uses.

10. DPIA Template and Tooling

10.1. The college of Wolverhampton college will maintain a DPIA template aligned to ICO criteria (with screening questions, risk matrix, and mitigation catalogue). Sector-grade public templates for example (NHS DPIA template) may be referenced for structure and completeness.

10.2. Linkages to Other Information Governance Framework

10.3. The College Information Asset Register (IAR): update upon DPIA sign- off

10.4. The College to ensure Vendor due diligence & contracts: Ensure Article 28 clauses, project security schedules, and audit rights reflect DPIA outcomes.

10.5. The college to ensure Security standard with all projects: Align with I.T security controls (encryption, identity/access, logging, incident response etc.).

10.6. The college to ensure Privacy notices & transparency align with DPIAs: Publish/update privacy information consistent with DPIA outcomes.

10.7. The college Incident/breach Management: Use DPIAs to inform preventive controls and breach frameworks.

11. Failure to complete a DPIA/Escalation

11.1. Failure to carry out a required DPIA May:

- The college will be in breach of UK Data protection Act 2018
- The college will be expose to regulatory enforcement and reputational damage.
- This can result in disciplinary action under ICO procedures.

11.2. Any residual high risk must be escalated to the EMT and if unresolved, to the ICO via the GDPR department (Article 36)

12. Documentation & record keeping

12.1. The GDPR contact person to store all DPIAs, screening forms, Advice, decision records, data sharing agreement, mitigation and action logs in the GDPR SharePoint with version controls.

12.2. The college is require retaining DPIAs for the life of processing plus seven (7) years, unless legal/sector requires the document to be kept longer.

12.3. The college to maintain an auditable trail demonstrating compliance and accountability and may be audited both internally and externally.

13. Training & Awareness

13.1. The GDPR department to carry out mandatory DPIA awareness for project leads, product owners, procurement, IT and data stewards.

13.2. Specialist training for those who author DPIAs; refresh at least every 24 months or upon major regulatory change

14. Monitoring/Review of the DPIA

14.1. The GDPR manager to sample completed DPIAs each quarter, track actions to closure, and report to EMT board.

14.2. The policy will be reviewed annually or upon significant changes in law or ICO guidelines.

15. Legal & Regulatory references

- **UK GDPR** (Articles 5, 25, 35–36; relevant recitals).
- **Data Protection Act 2018.** [legislation.gov.uk]
- **ICO Guidance:** “Data protection impact assessments (DPIAs). [ico.org.uk]