Data Protection Impact Assessment Procedure

Author:	**Data Protection Officer**	**Date:**	**February 2024**
Approved by:	**Information Governance Group**	**Approval Date:**	**February 2024**
Net Review Date	**February 2027**		

Purpose

This procedure provides specific operational guidance on the completion of Data Protection Impact Assessments as required by the Data Protection Policy and in order to demonstrate compliance with UK Data Protection Law.

The purpose of the procedure is:

- To ensure that staff with responsibility for designing, evaluating and updating processes, procedures, systems and reports that involve the processing of personal information fully understand the criteria for completion of a Data Protection Impact Assessment.
- To provide a framework for the completion of impact assessments in line with guidance from the Information Commissioner's Office, and taking into account the environment in which Trafford College and Stockport Group operates
- To provide a framework for appraisal, approval or referral, and regular review of data protection impact assessments as part of a wider framework of governance for information assets across the group.

Scope

This procedure applies to all personal data processing activities undertaken by Trafford and Stockport College Group (The Group) and therefore to all members of staff who are involved in the design, review or management of such activities, procedures and processes.

Responsibility

All Staff - responsible for identifying cases where changes they are making to policy, procedure, process or other activities (including projects and significant system changes) involving personal data about any individual may have an impact on those individuals, and ensuring that a Data Protection Impact Assessment is undertaken as an integral part of any such changes.

Data Link Co-ordinators and the Strategic Lead for Data Protection – responsible for providing initial support, guidance and knowledge to support the completion of Data Protection Impact Assessments as required. Responsible for the submission of draft assessments for review and feedback by the Data Protection Officer.

The Data Protection Officer – responsible for advising on all aspects of the DPIA process as required, supporting Data Link Co-ordinators with the completion of comprehensive assessments and providing advice to the Leadership Team prior to the approval of any change.

College Leadership and Executive Leadership Team – responsible for the approval of all changes where a DPIA has identified risks to the processing of personal data and any mitigations.

Procedure

1. General Principles

1.1 Data Protection Impact Assessment (DPIA) provides a clear framework to review and evaluate the impact of data processing on the data subject, identifying any possible adverse impact or deviation from the requirements of UK law, and a framework in which to manage specific risks.

1.2 Impact assessments will always be completed with support from a trained Data Protection Business Partner, and reviewed by the Data Protection Officer. Approval to implement changes assessed by an impact assessment will be given by the appropriate member of the Executive Leadership Team.

1.3 DPIAs consider data protection compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus should be on the potential for harm – to individuals or to society at large, whether it is physical, material or non-material.

2. When to conduct a DPIA

2.1 The Group conduct a DPIA as early as possible in a project's lifecycle.

2.2 The Group will conduct a DPIA when:

2.2.1 A DPIA is legally required. This is where the processing is likely to result in a high risk to individuals, and the project/processing:

- Uses systematic and extensive profiling or automated decision-making to make significant decisions about people.
- Process special-category data or criminal-offence data on a large scale.[1]
- Systematically monitors a publicly accessible place on a large scale.
- Uses innovative technology in combination with any of the criteria in the European guidelines.
- Uses profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit.
- Involves carrying out profiling on a large scale.
- Processing biometric or genetic data in combination with any of the criteria in the European guidelines.
- Involves combining, compare or match data from multiple sources.
- Processing personal data without providing a privacy notice directly to the individual in combination with any of the criteria in the European guidelines.
- Processing personal data in a way that involves tracking individuals' online or offline location or behaviour, in combination with any of the criteria in the European guidelines.
- Processing children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them.
- Processing personal data that could result in a risk of physical harm in the event of a security breach.

2.2.2 A DPIA is considered best practice. In line with the risk-based approach embodied by the GDPR; this is where the processing:

- Is part of any major project which requires the processing of personal data.
- Involves evaluation or scoring.
- Involves systematic processing of sensitive data or data of a highly personal nature.
- Includes any personal data on a large scale.
- Includes data concerning vulnerable data subjects.
- Uses innovative technological or organisational solutions.

- Prevents data subjects from exercising a right or using a service or contract.

3. Where Group decides not to carry out a DPIA, the reasons for not doing so will be documented.

3. Completing and Documenting DPIAs

3.1 All DPIAs will be completed using the Group's Microsoft Office Form on SharePoint, stored centrally in an electronic for future reference and review.

3.2 The impact assessment should be carried out by the person or department planning any change that falls within the scope of this procedure, and should include input from process and system specialists where appropriate, and external experts if required. The Data Protection Officer will support staff in completing the DPIA and the advice and recommendations of the Data Protection Officer will be recorded. Please also see Appendix 1 for a DPIA Screener which should help staff decide if a DPIA is needed.

3.3 All sections of the impact assessment should be considered and completed, using the examples and guidance included in the standard form. A DPIA will:

- Describe the nature, scope, context and purposes of the processing.
- Assess necessity, proportionality and compliance measures.
- Identify and assess risks to individuals.
- Identify any additional measures to mitigate those risks.
- Include the views of data subjects and other stakeholders where appropriate. If the views of Data Subjects are not sought Group should document its justification for not seeking the views of data subjects, for example if doing so would compromise the confidentiality of business plans, or would be disproportionate or impracticable.

4. Consultation

4.1 As part of all impact assessments, consideration should be given to the need to consult, and the decisions of which groups to consult, as well as the outcomes of consultation, clearly documented for future reference.

4.2 Where consultation identifies a high risk or a significant concern from representative potential data subjects, these should be clearly documented, brought to the attention of the Data Protection Officer, and if appropriate, discussed with the Information Commissioners office at an early stage in the process.

5. Risk Assessment

5.1 The assessment of risk and consideration of appropriate mitigations is a mandatory and significant element of the impact assessment process.

5.2 The risks associated with the project will be recorded in the DPIA, along with measures to mitigate the risks. These risks and any other associated actions will then be incorporated into departmental risk registers or into the overall planning for the project. The project must not start until mitigating measures are in place.

5.3 Where an assessment identifies an ongoing significant risk, this will be recorded as part of the department or Group risk register for further monitoring as appropriate. If high risk is identified that cannot be mitigated, the Group will consult the Information Commissioner's Office before starting the processing.

6. Approval, Referral and Escalation to the Information Commissioner's Office

6.1 All impact assessments will be reviewed and endorsed by the Data Protection Officer.

6.2 Approval to make changes as a result of an impact assessment will be given by the appropriate member of the Executive Leadership team.

6.3 Changes assessed as low risk will be reviewed by the Data Protection Officer as part of the routine approval process.

6.4 Medium risks will be discussed by the Data Protection Officer and appropriate member of the Executive Leadership Team before any approval is given, with consideration given to a facilitated discussion at an appropriate Executive Leadership Team meeting.

6.5 High Risk processing will not be authorised without prior approval from the Executive Leadership Team, review and approval by the Information Commissioners Office, and notification to the Audit Committee of the Corporation Board as part of a regular report on data protection matters.

Procedure Monitoring and Review

All impact assessments will be monitored in the 3 months following implementation of a change to ensure that a) actions and mitigations agreed as part of the process have been implemented and b) that no unintended consequences present new or increased risk.

The library of completed impact assessments will be reviewed annually to ensure that non require update or have become redundant due to a further change or end to processing arrangements.

APPENDIX 1

DPIA Screener - Do we need to carry out a Data Protection Impact Assessment (DPIA)?

It is a legal requirement where any data processing is likely to result in a high risk to individuals and good practice for any project involving the processing of personal data. A DPIA documents what data processing will be carried out and how any privacy or data protection risks will be addressed.

Even if a DPIA is not required, you will need to keep a record of what data processing you will be carrying out. This screener allows you to quickly highlight risks and identify whether you need to **do a DPIA** or where you can **continue** to the next stage of the screener.

It will also identify a **TO DO LIST**, other relevant actions that will be necessary, even if you do not need to progress to a formal DPIA.

Is it personal data?

If **YES**, **continue**. If **NO**, no need to continue with the screener or carry out a DPIA.

Is it a <u>new</u> activity/collection of personal data?

For example, you currently collect personal data on an IT system which conducts surveys, and you are only changing provider of the software (or renewing the contract) **NOT** collecting new personal data.

If **YES**, no need to continue with the screener or carry out a DPIA. **TO DO LIST** *Ensure a contract is in place including data protection clauses*

If **NO**, **continue**

Is it children's personal data?

YES - do a DPIA If **NO**, **continue**

Is it special category data?

(*special category data covers physical or mental health or condition, sexual life, religious / other beliefs, political opinions, trade union membership, biometric or genetic information used to identify an individual*)

YES – do a DPIA If **NO**, **continue**

Is it criminal offence data?

YES – do a DPIA If **NO**, continue

What is the legal basis for processing the data?

Which of the six available legal basis applies?

a) Data subject has given their **consent**
b) Data subject is party to a **contract** with you (the 'data controller')
c) You (the 'data controller') have a **legal obligation** to process the data
d) The data subject's **vital interests** are at stake and they cannot give consent
e) The processing is necessary for statutory or **public task** (public authorities only)
f) The data processing meets a **legitimate interest** for the you (the 'data controller') or another party

If you do not know **– do a DPIA** If you do know, **continue**

If the legal basis is consent, how is it obtained and where will you keep a record of it?

Consent needs to be it needs to be:

- **a clear affirmative action:** an "opt-in" rather than "opt-out"
- **fully informed:** people need to know what they are opting into, who will be storing their data and how
- **freely given:** there should be no power imbalance or implied pressure to provide the consent. The consent should be as easy to retract as it is to provide.
- **must be recorded:** the organisation should retain a record of the consent

Consent may not be the most appropriate legal basis.

Ensure you have a system to record all consent given (and withdrawn).

TO DO LIST Seek advice from the Data Protection Officer.

Will there be any Direct Marketing (e.g. a mailing list / promotions / telephone campaign) carried out as part of this project?

TO DO LIST *Ensure that Privacy and Electronic Communications Regulations (PECR) are covered*

Are we creating statistics or performance metrics from the data in addition to its primary function?

Ensure that figures do not identify individuals, lead to any individual interventions or cause damage and distress – if this is possible **do a DPIA**

Is there any solely automated profiling being carried out?

YES - do a DPIA NO – continue

Is this processing stated in the University privacy notices or is there existing privacy information for the data subject or do we need to take steps to inform them?

TO DO LIST *Check your privacy notices to see if this project is covered*

Data Protection - The Trafford & Stockport College Group (tscg.ac.uk)

If no or you do not know **– do a DPIA** If YES **continue**

Is there any new or inherently privacy-invasive technologies e.g., phone location or GPS?

YES – do a DPIA NO – continue

Is there any third-party hosting by a 'data processor'?

TO DO LIST *Ensure a contract is in place including data protection clauses*

Are there any third parties involved where an information sharing agreement is required (e.g. police, local authority)?

YES - do a DPIA

NO – continue

Is there a retention policy in place for the data?

TO DO LIST *Define how long you need the data for*

Will the data be stored outside the UK or EEA?

If **YES**, **continue**, if **NO do a DPIA**

Even if you do not need to carry out a DPIA, you should ensure that still fulfil your other obligations as a data controller.