Data Protection Screening and Impact Assessment Form

Decision/Project:	Neighbourhoods Department Approach.	DPO to add DPIA #.
Lead Officer:	Adam Parkinson	Neighbourhood Manager North
Head of Service (IAO):	Marion Walker	Head of Neighbourhoods

Any new decision or project involving 'high risks' must have a 'Data Protection Impact Assessment' (DPIA) carried out on it BEFORE any personal data is used. The Council can be fined up to £8.7million if it does not complete a DPIA when one was required.

Step 1: Screening Questions

Does the decision/project use any information **relating to living people** who can **be identified directly** from that data or **can be indirectly identified** if that data was put together with other information? Yes

If the answer is 'No' then data protection laws do not apply – stop here

Do any of the following apply to this decision/project:

- Data used in this way with no changes **since before 31 May 2018**. ☐
- Data use is **very similar** to an **existing DPIA** ADD MBC REFERENCE NUMBER. ☐
- The **Law states** a DPIA is **not required** ADD WEBLINK TO SPECIFIC LAW. ☐
- DPIA was done when **the Law** that supports the **data use was approved** ADD WEBLINK TO DPIA. ☐

If the answer to any of the above is 'Yes' then a DPIA is not needed – stop here

You must complete a DPIA if you answer 'YES' to any of these questions:

1. Large scale use of special category and/or criminal convictions or offences data. Yes
2. Systematic monitoring of a publicly accessible area on a large scale. No
3. Decisions based on automated decision-making (including profiling):
   - About access to a product, service, opportunity or benefit, or
   - Involving special category data, or
   - With legal or similar significant effect, or
   - With systematic and extensive evaluation with legal or other significant effects.

   No
4. Any profiling of individuals on a large scale. No
5. Combining, comparing or matching personal data obtained from multiple sources. Yes
6. Use of data that could jeopardise the physical health or safety of individuals if it were disclosed in a personal data breach. Yes

Step 1: Screening Questions	
You should *consider* completing a DPIA if you answer 'Yes' to <u>one</u> of these questions. **You *must* complete a DPIA if you answer 'Yes' to <u>two or more</u> of these questions.**	
7. Evaluation or scoring, profiling or predicting, especially aspects about performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements.	No
8. Observation, monitoring or control of individuals, including data collected through networks or a systematic monitoring of a publicly accessible area or tracking an individual's geolocation or behaviour, including but not limited to the online environment.	No
9. Special category or criminal convictions or offence information use or anything that could increase the possible risk to the rights and freedoms of individuals – especially biometric or genetic data.	Yes
10. Large scale use of any personal data either by number of individuals, volume, duration, or geographical extent.	Yes
11. Information about vulnerable individuals including children, adults, employees where there is an imbalance of power with the organisation.	Yes
12. Innovative use of or applying new technological or organisational solutions.	No
13. Preventing individuals from exercising a right or using a service or a contract as a result of use of their information.	Yes
14. Invisible processing where personal data that has not been obtained direct from the individuals and providing a privacy notice would prove impossible or involve disproportionate effort.	No

Justification for <u>not</u> completing a DPIA (if applicable)
, the Information Asset Owner for this project, has reviewed the screening question responses, acknowledged that they indicated that a DPIA is required, but decided on CHOOSE DATE not to progress this because **none of the questions above in section 1 had a 'yes' answer**.

Send the form with completed screening questions to:
dataprotection@middlesbrough.gov.uk.

It will then be checked and advice provided on your responses.

<u>Only complete the rest of this DPIA if the Data Protection Officer advises it is needed.</u>

Step 2: About the Decision/Project

This decision/project will ADD TEXT HERE**.**

The data will be collected from the individuals, existing records, and other organisations.

Data will be collected by **Appropriate Partners,** used to **support and achieve the strategic aims of the Neighbourhood Department,** stored in **secure systems in line with the appropriate organisations policies and procedures** , and then deleted or anonymised in line with retention periods for **each organisation.**

All data items will be collected on a an on-going basis.

Data will be shared with **Neighbourhood staff and partners** for the purposes of **the departments overarching strategic aims.**

The number of people affected may include 100,000+ within the area of Middlesbrough.

The individuals will be residents, business owners, and visitors of a service that they have some control over whether or not they receive or accept it. They will be able to refuse or withdraw consent, exercise GDPR rights, or contact to the DPO

It is believed that individuals would reasonably expect their data to be used in this way because it is accepted as part of service delivery.

The following groups may be affected by this data use:

- ☒ Children
- ☐ Employees
- ☒ Others in an imbalance of power i.e. Council decision-making power over a desired outcome.
- ☒ Mental health sufferer/reduced capacity
- ☒ Asylum seekers

Privacy concerns around this data use are not widespread. Security flaws relating to this data use are under regular review and controls adapted. The relevant approach/technology is CHOOSE AN ITEM.

The data use will achieve ADD TEXT HERE with the following benefits for the Council and more broadly: ADD TEXT HERE.

The National Data Opt-Out does not apply to this decision/project.

The Employee Protection Register is not affected by this decision/project.

Public consultation is not necessary. If relevant, consultation details, including by who and when responses were reviewed, if views were departed from, include: ADD TEXT HERE.

The following internal individuals or teams have been consulted as part of this assessment:

- ☒ Data Protection Officer
- ☒ ICT Services
- ☒ Legal Services
- ☒ HR Services
- ☒ Data Team
- ☒ CCTV Unit
- ☒ Staff Groups
- ☒ Trade Unions
- ☒ SMT/DMT/LMT
- ☒ Elected Members
- ☐ Suppliers
- ☒ ADD OTHERS

The data use will achieve the purpose. The alternatives to achieve the same outcome:

- ☐ Are cost prohibitive
- ☒ Fail to deliver the same outcomes
- ☐ Do not mitigate identified risks
- ☒ Conflict with legal/regulatory requirements

If data is transferred outside of the UK, by the Council or any supplier or their sub-contractors, it is sent to the following territories and protected with these measures:

Data	Territory	Protection Measure
ADD TEXT HERE	ADD TEXT HERE	CHOOSE AN ITEM
ADD TEXT HERE	ADD TEXT HERE	CHOOSE AN ITEM
ADD TEXT HERE	ADD TEXT HERE	CHOOSE AN ITEM

Step 2: About the Decision/Project		
The purposes and lawful basis for the data uses are:		
Purpose and Lawful Basis #1	**Purpose and Lawful Basis #2**	**Purpose and Lawful Basis #3**
Purpose	Purpose	Purpose
Personal Data	Personal Data	Personal Data
Special Category Data	Special Category Data	Special Category Data
Schedule 1 Condition	Schedule 1 Condition	Schedule 1 Condition
Criminal Convictions/Offences Data	Criminal Convictions/Offences Data	Criminal Convictions/Offences Data
Schedule 1 Condition	Schedule 1 Condition	Schedule 1 Condition
Supporting legislation or statutory guidance	Supporting legislation or statutory guidance	Supporting legislation or statutory guidance

Step 3: Risk Assessment and Controls									
List the risks and score them with NO controls in place.				**Set out the controls to reduce or eliminate risks and rescore them with controls in place.**					
Risk	**Likelihood of harm**	**Severity of harm**	**Overall risk**	**Options to reduce or eliminate risk**	**Effect on risk**	**Likelihood of harm**	**Severity of harm**	**Residual risk**	**Measures approved**
Inappropriate disclosure of personal data internally due to a lack of appropriate controls.	Almost Certain (5)	Extreme (7)	High (35)	☒ Data Protection Policy ☒ Secure Working Policy ☒ Incident Reporting and Management Procedure ☒ Staff Vetting Practices ☒ Physical and Environmental Security ☒ Mandatory Staff Data Protection and Security Training ☒ Device and Data Encryption ☒ Mandatory System User Training ☒ User Accounts and Passwords ☒ System Profiles and Permissions ☐ Compliance Checks on Contracts ☐ Data Processor Agreement with Contractor	Reduced	Rare (1)	Major (5)	Low (5)	Choose an item.
Accidental loss of electronic equipment may lead to risk of disclosure of personal information.	Almost Certain (5)	Major (5)	High (25)	☒ Data Protection Policy ☒ Secure Working Policy ☒ Agile and Home Working Policy ☒ Incident Reporting and Management Procedure ☒ User Accounts and Passwords ☒ Data Backups ☒ Device Blocking and Remote Erasure ☒ Removable Media Prohibited	Reduced	Rare (1)	Major (5)	Low (5)	Choose an item.
Breach of data held electronically due to a cyber-attack.	Almost Certain (5)	Extreme (7)	High (35)	☒ Secure Working Policy ☒ Incident Reporting and Management Procedure ☒ Mandatory Staff Cyber Security Training ☐ ICT Technical Security and Protection Measures ☒ Data Backups and Disaster Recover Plans ☒ Business Continuity Plans ☐ Compliance Checks on Contracts ☐ Data Processor Agreement with Contractor	Reduced	Rare (1)	Extreme (7)	Low (7)	Choose an item.
Vulnerable individuals or individuals affected by disclosure of special category or criminal offence data.	Almost Certain (5)	Extreme (7)	High (35)	☒ Data Protection Policy ☒ Secure Working Policy ☒ Mandatory Staff Data Protection and Security Training ☒ Device and Data Encryption ☐ Security Classification Scheme (Protective Marking) ☒ System Profiles and Permissions ☐ Compliance Checks on Contracts ☐ Data Processor Agreement with Contractor	Reduced	Rare (1)	Extreme (7)	Low (7)	Choose an item.
Information not anonymised effectively leading to personal data being disclosed.	Almost Certain (5)	Major (5)	High (25)	☒ Data Management Policy ☒ Data Standardisation Framework ☒ Mandatory Staff Data Protection and Security Training ☒ Data Minimisation Procedures ☒ Information Sharing Agreement ☐ Compliance Checks on Contracts ☐ Data Processor Agreement with Contractor	Reduced	Rare (1)	Major (5)	Low (5)	Choose an item.
Sharing pseudonymised data leads to unauthorised reidentification and personal data breaches.	Almost Certain (5)	Major (5)	High (25)	☒ Data Management Policy ☒ Data Standardisation Framework	Reduced	Rare (1)	Major (5)	Low (5)	Choose an item.

Step 3: Risk Assessment and Controls									
List the risks and score them with NO controls in place.				**Set out the controls to reduce or eliminate risks and rescore them with controls in place.**					
Risk	**Likelihood of harm**	**Severity of harm**	**Overall risk**	**Options to reduce or eliminate risk**	**Effect on risk**	**Likelihood of harm**	**Severity of harm**	**Residual risk**	**Measures approved**
				☒ Mandatory Staff Data Protection and Security Training ☐ Data Minimisation Procedures ☒ Information Sharing Agreement ☐ Compliance Checks on Contracts ☐ Data Processor Agreement with Contractor					
Personal data used in a manner or for purposes not anticipated by data subjects due to a change in the project.	Almost Certain (5)	Major (5)	High (25)	☒ Data Protection Policy ☒ Mandatory Staff Data Protection and Security Training ☐ Privacy Notice ☐ Data Protection Rights Procedure ☒ Information Sharing Agreement ☐ Compliance Checks on Contracts ☐ Data Processor Agreement with Contractor	Reduced	Unlikely (2)	Moderate (3)	Low (6)	Choose an item.
Sharing of personal data with other data controllers is not compliant or was not expected or reasonable to the individuals.	Almost Certain (5)	Major (5)	High (25)	☒ Data Protection Policy ☒ Mandatory Staff Data Protection and Security Training ☐ Privacy Notice ☐ Data Protection Rights Procedure ☒ Information Sharing Agreement	Reduced	Unlikely (2)	Moderate (3)	Low (6)	Choose an item.
Merging datasets may result in a data controller having far more information about individuals than anticipated by the individuals.	Almost Certain (5)	Major (5)	High (25)	☒ Data Protection Policy ☒ Data Management Policy ☒ Data Standardisation Framework ☒ Mandatory Staff Data Protection and Security Training ☒ Data Minimisation Procedures ☐ Privacy Notice ☐ Data Protection Rights Procedure ☒ Information Sharing Agreement ☐ Compliance Checks on Contracts ☐ Data Processor Agreement with Contractor	Reduced	Possible (3)	Moderate (3)	Medium (9)	Choose an item.
Technology capable of making visual or audio recordings or location tracking may be unacceptably intrusive.	Almost Certain (5)	Major (5)	High (25)	☒ Data Protection Policy ☒ Surveillance Policy ☒ Mandatory Staff Data Protection and Security Training ☐ CCTV Single Point of Contact Officer ☐ DPIA for Surveillance Camera Systems ☐ Mandatory System User Training ☐ User Accounts and Passwords ☐ System Profiles and Permissions ☐ Compliance Checks on Contracts ☐ Data Processor Agreement with Contractor	Reduced	Possible (3)	Moderate (3)	Medium (9)	Choose an item.
Collection of data containing identifiers may prevent users from using a space or service anonymously.	Almost Certain (5)	Moderate (3)	Medium (15)	☒ Data Protection Policy ☒ Surveillance Policy ☐ Data Protection by Design Process ☐ Data Minimisation Procedures	Reduced	Unlikely (2)	Moderate (3)	Low (6)	Choose an item.
Collection of unnecessary data if appropriate policies not in place, leading to unnecessary risks.	Almost Certain (5)	Major (5)	High (25)	☒ Data Protection Policy ☒ Data Management Policy ☒ Data Standardisation Framework ☒ Mandatory Staff Data Protection and Security Training	Reduced	Unlikely (2)	Moderate (3)	Low (6)	Choose an item.

Step 3: Risk Assessment and Controls									
List the risks and score them with NO controls in place.				**Set out the controls to reduce or eliminate risks and rescore them with controls in place.**					
Risk	**Likelihood of harm**	**Severity of harm**	**Overall risk**	**Options to reduce or eliminate risk**	**Effect on risk**	**Likelihood of harm**	**Severity of harm**	**Residual risk**	**Measures approved**
				☐ Data Protection by Design Process ☐ Data Minimisation Procedures ☐ Privacy Notice ☐ Data Protection Rights Procedure ☐ Compliance Checks on Contracts ☐ Data Processor Agreement with Contractor					
Data quality is poor leading to misidentification, decisions, service errors or failures, or personal data breaches.	Almost Certain (5)	Major (5)	High (25)	☒ Data Protection Policy ☒ Records Management Policy ☒ Data Management Policy ☒ Data Standardisation Framework ☒ Mandatory Staff Data Protection and Security Training ☐ Quality Audit Procedure for Business Processes ☐ Compliance Checks on Contracts ☐ Data Processor Agreement with Contractor	Reduced	Possible (3)	Moderate (3)	Medium (9)	Choose an item.
Data may be kept longer than required in the absence of appropriate policies or procedures.	Almost Certain (5)	Moderate (3)	Medium (15)	☒ Data Protection Policy ☒ Records Management Policy ☒ Records Retention and Disposal Schedules ☒ Records Manager Advice ☒ Records Management Audit Programme ☐ System Records Retention and Disposal Procedures ☐ Compliance Checks on Contracts ☐ Data Processor Agreement with Contractor	Reduced	Unlikely (2)	Moderate (3)	Low (6)	Choose an item.
Data may be stored in a legacy system that is still in current use or may not be disposed of at the proper time.	Almost Certain (5)	Moderate (3)	Medium (15)	☒ Data Protection Policy ☒ Records Management Policy ☒ Records Retention and Disposal Schedules ☒ Records Management Audit Programme ☒ Data Migration Plan ☐ Records Digitisation Plan ☐ Compliance Checks on Contracts ☐ Data Processor Agreement with Contractor	Reduced	Unlikely (2)	Moderate (3)	Low (6)	Choose an item.
Inability to exercise rights (including but not limited to privacy rights).	Almost Certain (5)	Major (5)	High (25)	☒ Data Protection Policy ☒ Mandatory Staff Data Protection and Security Training ☒ Data Protection Officer ☒ Publication of Rights and Contact Information ☐ Privacy Notice ☐ Data Protection Rights Procedure ☐ Compliance Checks on Contracts ☐ Data Processor Agreement with Contractor	Reduced	Rare (1)	Major (5)	Low (5)	Choose an item.
Financial loss or other significant economic or social disadvantage	Almost Certain (5)	Major (5)	High (25)	☒ Data Protection Policy ☒ Incident Reporting and Management Procedure ☒ Data Protection Officer ☒ Publication of Rights and Contact Information ☐ Privacy Notice ☐ Equalities Impact Assessment ☐ Quality Audit Procedure for Business Processes	Reduced	Possible (3)	Moderate (3)	Medium (9)	Choose an item.

Step 3: Risk Assessment and Controls									
List the risks and score them with NO controls in place.				**Set out the controls to reduce or eliminate risks and rescore them with controls in place.**					
Risk	**Likelihood of harm**	**Severity of harm**	**Overall risk**	**Options to reduce or eliminate risk**	**Effect on risk**	**Likelihood of harm**	**Severity of harm**	**Residual risk**	**Measures approved**
Data may be transferred to countries with inadequate data protection regimes.	Possible (3)	Extreme (7)	High (21)	☒ Data Protection Policy ☐ Data Transfer Impact Assessment ☐ Compliance Checks on Contracts ☐ Data Processor Agreement with Contractor	Reduced	Rare (1)	Moderate (3)	Low (3)	Choose an item.
Incorrect understanding and implementation of information governance laws by services and partners leading to non-compliance or services/project failures.	Almost Certain (5)	Extreme (7)	High (35)	☒ Data Protection Policy ☒ Mandatory Staff Data Protection and Security Training ☐ Consultation with Subject Matter Experts ☐ Data Protection by Design Process ☐ Information Sharing Agreement ☐ Compliance Checks on Contracts ☐ Data Processor Agreement with Contractor	Reduced	Unlikely (2)	Minor (2)	Low (4)	Choose an item.
Data processors fail to comply with legislation, contract specifications, or go outside of processing instructions.	Almost Certain (5)	Major (5)	High (25)	☐ Data Protection by Design Process ☐ Compliance Checks on Contracts ☐ Data Processor Agreement with Contractor	Reduced	Rare (1)	Minor (2)	Low (2)	Choose an item.
Data is not extractable from system during de-commissioning and is unavailable in line with retention periods	Almost Certain (5)	Extreme (7)	High (35)	☐ Consultation with Subject Matter Experts ☐ Data Protection by Design Process ☐ Data Migration Plan ☐ Records Digitisation Plan ☐ Data Migration Plan ☐ Records Digitisation Plan	Reduced	Rare (1)	Minor (2)	Low (2)	Choose an item.

Step 4: Sign-off and Outcomes

CHOOSE AN ITEM gave advice on this DPIA on CHOOSE DATE which included ADD TEXT HERE.

The Data Protection advice was accepted by **Adam Parkinson** on 22/10/2025.

If applicable, the advice was partially/wholly rejected because ADD TEXT HERE.

ADD TEXT HERE, the System Owner for this decision/project, has reviewed the contents of the assessment on 22/10/2025 and undertaken to ensure that all outstanding risk controls are implemented **before** the data use begins.

Marion Walker, the responsible officer for this decision/project, will review this assessment by 23/10/2025.

Next Section for Strategy Information and Governance Service use only.

CHOOSE AN ITEM reviewed this assessment on CHOOSE DATE and accepted the residual risks identified.

Additional notes: ADD TEXT HERE

If any residual 'high' risk is accepted, you must inform the Data Protection Officer who is required by law to report this assessment for consideration by the Information Commissioner's Office who can take 8 to 14 weeks to respond.

The following appendices should be considered alongside this assessment:
ADD TEXT HERE