APPENDIX 1

Appropriate Policy Processing Special Category Data/Criminal Conviction Data

Date: July 2021

Version: V3.0

Document Version Control

Document Version Control	
Issue Number	Date
1.0	16 April 2021 – Considered by Information Governance Group
2.0	15 May 2021 – Considered by Information Governance Champions Group
3.0	27 July 2021 – Audit Panel for Approval

This is a live document effective from the issue date. It supersedes any previous versions of this document, which are now withdrawn.

Contents

1. Introduction

1.1 In order for Tameside Council (the Council) to carry out its statutory and public functions, we process special category data and criminal offence data in accordance with the requirements of Article 9 and 10 of the UK General Data Protection Regulation (UK GDPR) and Schedule 1 of the Data Protection Act 2018 (DPA 2018).

1.2 This policy applies when the Council is processing special category data when relying on the requirements listed in Parts 1, 2 and 3 of Schedule 1 of the Data Protection Act 2018. This policy lists the procedures, which are in place to secure compliance with the UK General Data Protection Regulation and data protection principles, needed when processing special category data.

2. Scope

2.1 This policy applies to all personal information including special category/criminal conviction data used, stored or shared by or with the Council whether in paper or digital form and wherever it is located. It also applies to all personal information and special category information processed by the Council on behalf of other organisations. Personal data is defined as:
'any information relating to an identified or identifiable individual; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number (e.g. social security number) or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity (e.g. name and first name, date of birth, biometrics data, fingerprints, DNA…)'.

2.2. This policy applies to all Council employees, seconded staff members, volunteers, third party contractors, temporary staff and employees of other organisations who directly or indirectly support Council services.

2.2. This policy also sets out how special category and criminal convictions personal data will be protected in line with Schedule 1 of the DPA 2018.

2.3. This policy applies to data processing where the Council is a data controller in its own right or is a data controller in relation to a multi-agency data sharing partnership. This policy also applies when the Council is acting as a Data processor on behalf of one or more data controllers.

3. Policy Statement

3.1. Data Protection legislation governs how the Council will process personal and special category data including where applicable criminal conviction data collected from members of the public, current, past and prospective employees, clients and customers, law enforcement and other agencies.

3.2. This policy states how the Council will comply with Data Protection legislation to ensure that all the personal data held is collected, stored and used appropriately.

4. Roles and Responsibilities

4.1. Chief Executive

The Chief Executive is ultimately responsible for the organisation's compliance with data protection legislation. Part 7 of the DPA 2018 stipulates the Chief Executive's liability with regards to offences committed under the Act.

4.2. Monitoring Officer

The Monitoring Officer is responsible for ensuring the lawfulness and fairness of Council decision making and must report on matters they believe are, or are likely to be, illegal or amount to maladministration. They are also responsible for matters relating to the conduct of members and officers. The Council's Director of Governance and Pensions (Borough Solicitor) is the Monitoring Officer.

4.3. Senior Information Risk Owner (SIRO)

The SIRO has an overall strategic responsibility for governance in relation to data protection risks and is responsible for:

- Acting as an advocate for managing information risk within the Council championing and fostering a culture that values, protects and uses information for the success of the organisation and benefit of its customers;
- Owning the organisation's overall information risk policy and risk assessment processes and ensuring they are implemented consistently by IAOs;
- Providing written advice to the Council on the content of their annual governance statement in regard to information risk; and
- Owning the organisation's Information Incident Procedure and Practice Note. The SIRO for the Council is the Head of Risk Management and Audit.

4.4. Data Protection Officer (DPO)

Under the Data Protection Legislation all public authorities must appoint a DPO. The DPO is responsible for:

- Informing and advising the Council and its employees of their data protection obligations.
- Monitoring compliance with the Data Protection legislation and internal data protection policies and procedures.
- Monitoring the assignment of responsibilities, awareness training, and training of staff involved in processing operations and related audits.
- Advising on whether a DPIA (data protection impact assessment) is necessary, how to conduct one and expected outcomes.
- Acting as the contact point for the supervisory authority (Information Commissioners Office) on all data protection issues, including data breach reporting.
- Serving as the contact point for data subjects e.g. employees, customers on privacy matters, including DSARs (data subject access requests).
- The Council will meets its obligations regarding the DPO role and as such will ensure that:
    - The DPO is involved, closely and in a timely manner, in all data protection matters;
    - The DPO reports to/is part of the highest management level of your organisation, i.e. board level at the Council this is the Single Leadership Team;
    - The DPO operates independently and is not dismissed or penalised for performing their tasks;
    - Adequate resources (sufficient time, financial, infrastructure, and, where appropriate, staff) is provided to enable the DPO to meet their GDPR obligations, and to maintain their expert level of knowledge;
    - The DPO has the appropriate access to personal data and processing activities; and
    - Appropriate access to other services within your organisation so that they can receive essential support, input or information. The Data Protection Officer for the Council is the Monitoring Officer.

4.5. Information Asset Owners (IAOs)

Information Asset Owners (IAOs) are members of the Extended Leadership Team. Their role is to understand in their business area what information is held, what is added and what is

removed, how information is moved, and who has access and why. The IAO is responsible for:

- Ensuring they understand and address risks to the information;
- Ensure that information is fully used within the law for the public good; and
- Providing a written judgement of the security and use of their asset annually to support the audit process.

4.6. Information Asset Administrators (IAA)

An IAO is accountable for the information assets under their control but may delegate day to day management responsibility to an IAA who would be responsible for:

- Managing the joiners, movers and leavers process within the team which may cut across the organisation and partner boundaries;
- Ensuring all team members keep their training up-to-date
- Managing the day to day security of the asset including access control management
- Identifying potential or actual security incidents and consulting the IAO on incident management
- Ensuring that risk assessments and other documents for projects are accurate and maintained
- Keeping and regularly reviewing records of Processing Activity
- Management of Information Asset Register (IAR)
- Act as gatekeeper ensuring that the Information Asset Owner is aware of any changes to the information asset or its use

4.7. Information Security Officer/Cyber Security Technical Specialist

The Information Security Officer and Cyber Security Technical Specialist are responsible for developing and implementing the Council's Cyber Strategy and Information Security and associated policies and procedures to reflect local and national standards and guidance and legislative requirements. They also support the Council in ensuring compliance with information security requirements. This important role is managed by the Assistant Director Digital Tameside.

4.8. Heads of Department will:

- Ensure all managers are made aware of this policy and understand their duties to ensure compliance across their teams;
- Notify the Information Governance Team and seek advice where activities involve the use of personal data. This includes any new projects, new data processing or any changes to existing processing;
- Ensure compliance with UK GDPR and Data Protection Legislation for all teams within their area; and
- Ensure all employees are appropriately trained in the safe handling and use of information and as a minimum complete the Council's data protection training every year.

4.9. Line managers will:

- Ensure that their teams are made aware of this policy and understand its requirements;
- Fully implement the requirements of this policy within their teams; and
- Ensure all employees are appropriately trained in the safe handling and use of information and as a minimum completed the Council's data protection training every year.

4.10. All staff must:

- Follow this policy for all processing of personal data throughout the Council;
- Protect any personal data within their care;

- Seek additional advice and guidance from their manager, Information Governance Team or the Data Protection Officer if unsure or in any doubt about how to handle personal information;
- Report any suspected or actual data breaches or any breaches of this policy to their line manager or the Information Governance team as soon as they become aware in line with the Information Incident Procedure and Practice Note; and
- Keep up to date with all Council Data Protection and Information Governance training that is appropriate to their role.

4.11. Information Governance Team will:

- Will be the source of subject matter expertise in relation to data protection;
- Develop and inform strategies in relation to the use of personal data;
- Provide strategic oversight to large scale programmes of personal data sharing;
- Will advise on and provide support in relation to data protection and the handling and use of personal data;
- Will provide guidance and support to staff undertaking Data Protection Impact Assessments;
- Develop and maintain relevant policies and procedures in line with changes to legislation and best practice;
- Manage and monitor requests from Data Subjects who choose to exercise their individual rights including Subject Access Requests in line with Council policies and procedures;
- Manage and monitor any Information Security Incidents/Breaches in line with the Councils Information Security Incident Procedure.; and
- Develop and deliver training as required.

5. Special Category Data

The UK GDPR defines Special Category Data as personal data that reveals:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric data for the purpose of uniquely identifying a natural person;
- Data concerning health; or
- Data concerning a natural person's sex life or sexual orientation.

6. Criminal Conviction Data

6.1 While not formally defined as special category data similar additional conditions and requirements also apply to criminal convictions and offences or related to security measures under Article 10 UK GDPR.

6.2 Section 11(2) of the DPA 2018 specifically confirms that this includes personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing. When processing such data the Council will ensure the relevant additional conditions and requirements are met.

7. This Policy Document

7.1 Under DPA 2018, there is a requirement for an Appropriate Policy Document to be in place when processing special category and criminal offence data under certain conditions. This document fulfils that requirement and should be read together with the Council's Information Governance Policy.

7.2 This document explains our procedures and compliance with the principles in Article 5 UK GDPR and our policies in relation to retention and erasure of this personal data. The document also explains our processing and satisfies the requirements of Schedule 1, Part 4 of the DPA 2018. In addition, it provides some further information about our processing of special category and criminal offence data where a policy document is not a specific requirement. The information supplements our corporate privacy notice which can be viewed here and the related service specific privacy notices.

7.3 The policy applies to all Council staff. "Staff" for the purposes of this policy includes Council officers, including contractors, consultants, interims and agency staff.

8. Conditions for processing special category and criminal offence data

8.1 Schedule 1 of DPA 2018 establishes conditions that permit the processing of the special categories of personal data and criminal convictions data. The Council in the processing of such data rely on the following conditions:

Part 1 – Conditions relating to employment, social security and social protection

The Council will process:

- Personal data concerning health in connection with our obligations under employment law and to support employees in their work environment.
- We may also process data relating to criminal convictions under Article 10 UK GDPR in connection with our obligations under employment law in connection with recruitment, disciplinary processes or dismissal.
- Examples of processing include staff sickness absences and political activity declarations.

Part 2 – Substantial Public Interest Conditions

Statutory etc. and government purposes

- Fulfilling obligations under UK legislation for the provision, evaluation and financial/contractual monitoring of services funded by the Council for residents within the Borough.
- Complying with other legal requirements, such as the requirement to disclose information in connection with legal proceedings.

Equality of opportunity or treatment

- Ensuring compliance with the Council's obligations under legislation such as the Equality Act 2010.
- Ensuring that we fulfil our public sector equality duty when carrying out our work.
- Ensuring we provide equal access to our services, to all sections of the community in recognition of our legal and ethical duty to represent and serve communities.

Preventing or detecting unlawful acts

- Processing data concerning criminal records in connection with employment in order to reduce the risk to the Council.
- Carrying out enforcement action in connection with the Council's statutory duties.
- Protecting the public against dishonesty etc.

- Processing data concerning dishonesty, malpractice, or other improper conduct in order to protect the residents of Tameside.
- Carrying out enforcement action in connection with the Councils statutory duties, like the Regulatory Reform (Fire Safety) Order 2005
- Carrying out investigations and disciplinary actions relating to our employees.
- Regulatory requirements relating to unlawful acts and dishonesty etc.
- Complying with the Council's enforcement obligations under UK legislation, like the Regulatory Reform (Fire Safety) Order 2005.
- Assisting other authorities in connection with their regulatory requirements.

Preventing fraud

- Disclosing personal data in accordance with arrangements made by an anti-fraud organisation.

Support for individuals with a particular disability or medical condition

To provide services or raise awareness of a disability or medical condition in order to deliver services to service users and their carers.

Counselling

For the provision of confidential counselling, advice or support or of another similar service provided confidentially.

Safeguarding of children and individuals at risk

- Protecting vulnerable children and individuals from neglect, physical, mental or emotional harm.
- Identifying individuals at risk whilst providing services and/or attending emergency incidents.
- Obtaining further support for children and individuals at risk by sharing information with relevant agencies.

Safeguarding of economic well-being of certain individuals

- To protect the economic wellbeing of an individual at economic risk who is aged 18 or over.
- Identifying individuals at risk whilst providing services and/or attending emergency incidents.
- Data sharing with our partners to assist them to support individuals.

Insurance

- Information that is necessary for insurance purposes.

Occupational pensions

- Fulfilling the Council's obligation to provide an occupational pension scheme.
- Determining benefits payable to dependents of pension scheme members.

Part 3 – Additional Conditions Relating to Criminal Convictions, etc.

Extension of conditions in Part 2 of Schedule 1 DPA 2018 referring to substantial public interest.

The Council may process personal data relating to criminal convictions in connection with its service obligations or as part of recruitment and employment checks to protect the public against dishonesty.

9. Procedures for Ensuring Compliance with the Principles

Accountability principle

9.1 The UK GDPR states that the data controller must be responsible for, and be able to demonstrate, compliance with these principles. The Data Protection Officer and Senior Information Risk Owner are responsible for ensuring that the Council is compliant with these principles.

9.2 The Council will:

- Ensure that records are kept of all personal data processing activities and that these are provided to the Information Commissioner on request;
- Carry out a Data Protection Impact Assessment for any high risk personal data processing and consult the Information Commissioner if appropriate;
- Appoint a Data Protection Officer to provide independent advice and monitoring of the Council's personal data handling and that this person has access to report to the highest management level of the department;
- Have in place internal processes to ensure that personal data is only collected, used or handled in a way that is compliant with data protection law;
- All employees receive annual data protection and information security training;
- Maintain logs of security incidents, data protection rights requests and details on information sharing with partners; and
- Maintain a data protection policy that sets out how we will ensure we meet our obligations under the UK GDPR and DPA 2018.

Principle 1: Lawfulness, Fairness and Transparency

9.3 Processing personal data must be lawful, fair and transparent. It is only lawful if and to the extent it is based on law and either the data subject has given their consent for the processing, or the processing meets at least one of the conditions in Schedule 1 DPA 2018.

9.4 The Council will:

- Ensure that personal data is only processed where a lawful basis applies;
- Only process personal data fairly, and will ensure that data subjects are not misled about the purposes of any processing; and
- Ensure that data subjects receive details on why we use and collect their data by providing privacy notices for services, so that any processing of personal data is transparent, as well as being clear and easy to understand.

9.5 Our processing for purposes of substantial public interest is necessary for the exercise of a function conferred on the Council by an Order or any other enactment (whenever passed or made).

9.6 Our processing for the purposes of employment relates to our obligations as an employer.

9.7 We also process special category personal data to comply with other obligations imposed on the Council in its capacity as a public authority e.g. the Equality Act 2010.

Principle 2: Purpose Limitation

9.8 Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

9.9 The Council will:

- Only collect personal data for specified, explicit and legitimate purposes, and we will inform data subjects what those purposes are in a privacy notice;

- Not use personal data for purposes that are incompatible with the purposes for which it was collected. If we do use personal data for a new purpose that is compatible, we will inform the data subject first; and
- If we are sharing data with another controller, document that they are authorised by law to process the data for their purpose.

9.10 We process personal data for purposes of substantial public interest when the processing is necessary for us to fulfil our statutory/public functions, where it is necessary for complying with or assisting another to comply with a regulatory requirement.

9.11 The Council is authorised by law to process personal data for these purposes. We may process personal data collected for any one of these purposes (whether by us or another controller), for any of the other purposes here, providing the processing is necessary and proportionate to that purpose.

Principle 3: Data Minimisation

9.12 The Council will only collect data that is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. The Council will only collect the minimum personal data that we need for the purpose for which it is collected.

9.13 Where personal data is provided to us or obtained by us, but is not relevant to our stated purposes, this will be erased.

Principle 4: Accuracy

9.14 The Council will ensure that personal data is accurate, and kept up to date where necessary. We will take particular care to do this where our use of the personal data has a significant impact on individuals.

9.15 Where the Council becomes aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure that data is erased or rectified without delay. If we decide not to either erase or rectify it, for example because the lawful basis we rely on to process the data means these rights don't apply, we will document our decision.

Principle 5: Storage Limitation

9.16 Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

- The Council will only keep personal data in identifiable form for as long as is necessary for the purposes for which it is collected, or where we have a legal obligation to do so. Once we no longer need personal data, it shall be deleted or rendered permanently anonymous. The Council will maintain appropriate Data Retention and Disposal Policies and Schedules.
- Retention periods are set out in our Retention and Disposal Schedules and are published in our Privacy Notices.
- Retention periods are based on legal requirements to retain data and consideration of the needs of data subjects through data protection impact assessments.

Principle 6: Integrity and Confidentiality (security)

9.17 Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

9.18 The Council will ensure that there are appropriate organisational and technical measures in place to protect personal data.

- We adhere to the Government's Minimum Cyber Security Standards and implements information security controls in line with Public Sector Network, Payment Card Industry and the NHS Data Security and Protection Toolkit.
- The Information Governance Group meets regularly to ensure suitable information governance is deployed throughout the Council.
- Technical security controls such as encryption are employed to secure sensitive information within systems.
- Role-based access controls are implemented to restrict access to sensitive data.
- Where possible, anonymisation or pseudonymisation techniques are used to reduce the risk of sensitive data being compromised.
- Retention and Disposal Policies are in place to ensure data is retained in line with agreed retention periods, and securely disposed of when appropriate.
- We retain personal information only for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

9.19 We will ensure, where special category or criminal convictions personal data is processed, that:

- There is a record of that processing, which complies with the requirements of Article 30 GDPR and paragraph 41 of Schedule 1 of the DPA and that record will set out, where possible, the envisaged time limits for erasure of the different categories of data;
- Where we no longer require special category or criminal convictions personal data for the purpose for which it was collected, we will delete it or render it permanently anonymous;
- We ensure all contracts with data processors include clauses regarding the exit of the contract and the return or destruction of any personal data processed.
- Data subjects receive full privacy information about how their data will be handled, and that this will include the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.
- We retain personal information only for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

10. Review Date

10.1 This policy will be retained for the duration of our processing and for a minimum of 6 months after processing ceases.

10.2 This policy will be reviewed annually or revised more frequently if necessary such as if there are any changes in legislation.

11. Data Protection Officer

Sandra Stewart – Director of Governance and Pension (Borough Solicitor)
Tameside One, Market Place. Ashton-under-Lyne. Tameside, OL6 6BH.
Email: information.governance@tameside.gov.uk

12. General Enquires

Information Governance Team
Tameside One, Market Place. Ashton-under-Lyne. Tameside, OL6 6BH.
Email: information.governance@tameside.gov.uk

13. Training

13.1 The Council will provide relevant training both online and face to face to ensure that staff understand the legislation and its application to their role.

13.2 All staff must complete mandatory data protection training every year and undertake any further training provided by the Council to enable them to perform their duties appropriately.

14. Compliance and Monitoring

14.1. Completion of training will be monitored by the Information Governance Team and all employees must have regard to data protection legislation and this policy when collecting, accessing, using, disclosing or destroying personal information. Failure to do so may result in disciplinary action and legal prosecution.

14.2 If an employee is in any doubt about how to handle personal information, they should speak to their line manager or contact the Information Governance Team.
Email: information.governance@tameside.gov.uk

14.3 Staff are responsible for informing the Information Governance Team of any new processing or changes to existing processing of personal data within their area. This will help the Council to meet the requirements of the legislation.

14.4 This policy will be reviewed at regularly by the Information Governance Team to ensure that it is updated in line with any change in legislation.

14.5 The Council will continue to review the effectiveness of this policy to ensure that it is achieving the intended purpose.