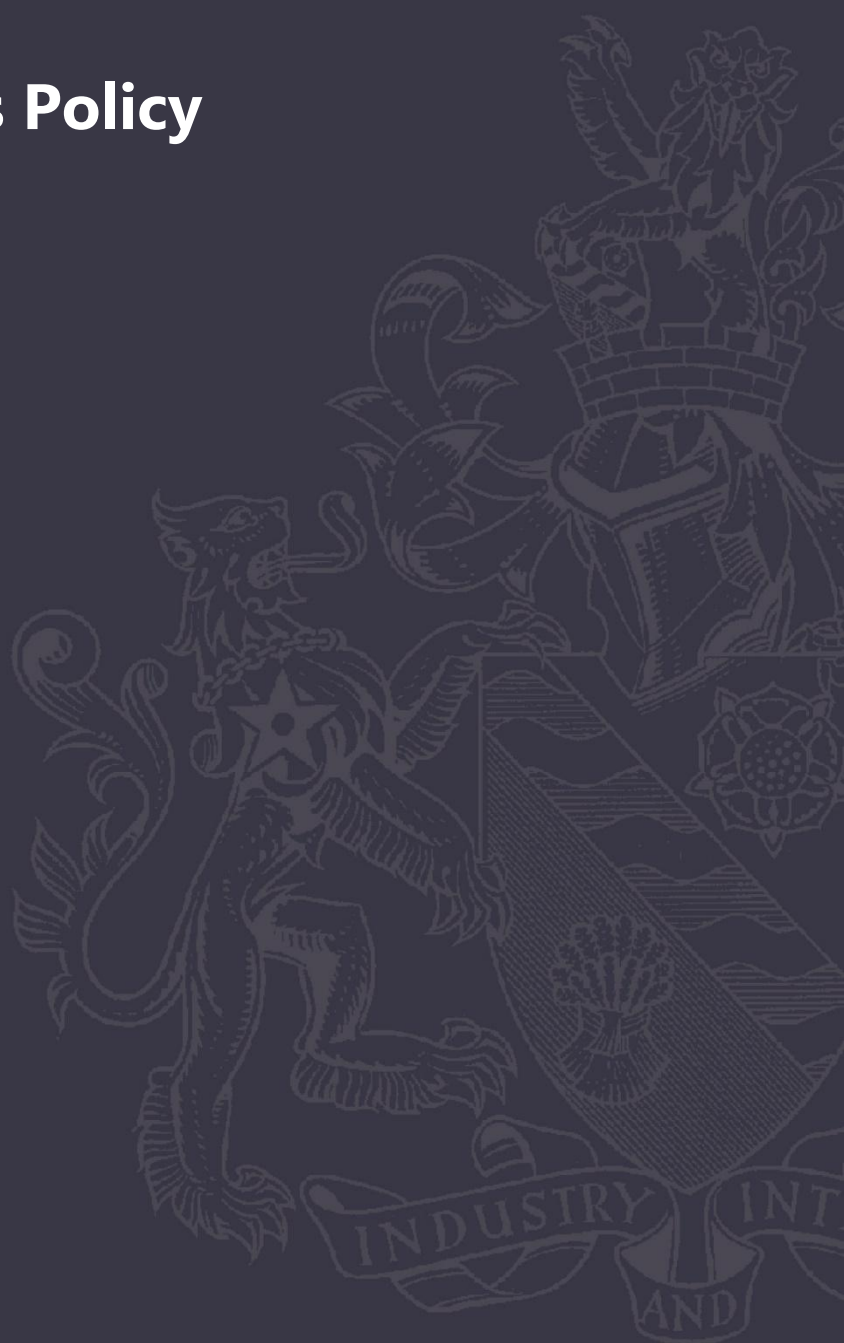


Individual's Rights Policy

April 2026



Document Control

Owner	Head of Information Governance & Data Protection Officer
Author	Information Governance Team
Last Reviewer	Head of Information Governance & Data Protection Officer
Approver	Executive Cabinet
Date of Approval	22 April 2026
Date of Next Review	April 2027
Version	1.0
Classification	Public

Version Number	Date	Changes	Approved by
1.0	April 2026	Original document (Replaces SAR Policy v1.0)	Executive Cabinet

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 It supersedes any previous version of this document, which are now withdrawn.

Further information, advice or guidance about this document can be obtained from:
The Information Governance Team
information.governance@tameside.gov.uk

Contents

1. INTRODUCTION	4
2. POLICY SCOPE	4
3. POLICY STATEMENT	4
4. ROLES AND RESPONSIBILITIES	5
5. INTRODUCTION TO DATA SUBJECT RIGHTS	5
6. WHAT ARE THE DATA SUBJECT RIGHTS?	5
7. RIGHT TO BE INFORMED	6
8. RIGHT OF ACCESS	7
9. RIGHT TO RECTIFICATION	8
10. RIGHT TO OBJECT TO PROCESSING	8
11.10. National Data opt-out	10
11. RIGHT TO RESTRICTION OF PROCESSING	11
12. RIGHT TO ERASURE ('RIGHT TO BE FORGOTTEN')	12
13. RIGHT TO DATA PORTABILITY	13
14. RIGHTS RELATING TO AUTOMATED DECISION MAKING	14
15. HOW INDIVIDUALS CAN EXERCISE THESE RIGHTS	15
16. TRAINING	21
17. TIME SCALES AND ESCALATION	21
18. COMPLIANCE AND MONITORING	23
20. CONTACT DETAILS	23
APPENDIX 1: Definitions	24
APPENDIX 2: Related Policies and Procedures	25
APPENDIX 3: Legislative Framework	26
Online Resources	26

1. Introduction

- 1.1. In order to fulfil its functions and duties Tameside Metropolitan Council (the Council) collects and processes personal data relating to individuals who use the services it provides, past, present and prospective employees, contractors, suppliers, clients, and others with whom it communicates.
- 1.2. This policy therefore sets out how the Council will comply with the Data Protection legislation in order to ensure that data subject rights are adhered to.
- 1.3. Any breach of this policy may result in disciplinary action and prosecution.

2. Policy 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.

- 2.2. 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...)

- 2.3. This policy applies to all TMBC employees, seconded staff members, elected members/councillors, volunteers, third party contractors, temporary staff and employees of other organisations who directly or indirectly support Council services.

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 data subject rights are adhered to.

4. Roles and responsibilities

- 4.1. Roles and responsibilities for defined data protection related roles and for all staff are set out in the accompanying Information Governance Roles and Responsibilities document.

5. Introduction to data subject rights

- 5.1. The rights of individuals ('data subjects') in relation to the processing of their personal information are set out in data protection legislation.
- 5.2. The [UK General Data Protection Regulations](#) (UK GDPR) and [Data Protection Act 2018](#) (DPA 2018) strengthened rights which already existed in UK law. The changes are mostly evolutionary but also give individual's rights in other areas such as the right to data portability. Some of these rights are subject to limitations and exceptions; further details of which may be viewed below.
- 5.3. This guidance provides an introduction to the rights individuals have under the data protection legislation.

6. What are the data subject rights?

- The right to be informed - The right to be provided with specified information about the processing of their personal data.
- The right of access - The right to access their personal data and certain supplementary information.
- The right to rectification - The right to have their personal data rectified, if it is inaccurate or incomplete.
- The right of erasure / right to be forgotten - The right to have, in certain circumstances, their personal data deleted or removed.
- The right to restriction - The right, in certain circumstances, to restrict the processing of their personal data.
- The right of data portability - The right, in certain circumstances, to move personal data the individual has provided to the Council to another organisation.
- The right to object - The right, in certain circumstances, to object to the processing of their personal data and, potentially, require the Council to stop processing that data.

- Rights related to automated decision making and profiling - The right to not be subject to decision-making based solely on automated processing.

- 6.1. These rights are not absolute and are subject to conditions and exemptions.
- 6.2. In some cases the rights described above only apply if the processing activity is undertaken on specific legal grounds and/or in defined circumstances. Therefore, these rights are unlikely to be engaged in all cases.
- 6.3. Individuals can also obtain full information about their rights from the Information Commissioner's Office (the ICO) via their website:
<https://ico.org.uk/for-the-public/>.
- 6.4. The ICO is the UK's independent regulator responsible for upholding and enforcing the rights of individuals under data protection law.
- 6.5. Where an individual exercises their individual rights listed above, the Council will respond without undue delay and in any event within one calendar month, subject to the following two exceptions:
 - Further time may be necessary, taking into account the complexity and the number of the request(s) from the individual, the period for responding may be extended by up to two further calendar months. Where such an extension is required The Council will notify the individual that this is the case within one calendar month of receiving their request.
 - Where the request(s) from an individual are manifestly unfounded The Council may refuse the request(s). In exceptional cases a reasonable fee may be requested that takes into account the administrative cost of complying with the request.

7. Right to be informed

- 7.1. [Article 13 UK GDPR](#) and [Article 14 UK GDPR](#) set out the obligations on the Council around providing data subjects with information about how the Council uses or intends to use their personal data. This
- 7.2. The Council will ensure that:
 - where we collect personal data from the individual we will provide them with, at the time the personal data is collected, specified 'fair processing' information (known as a 'privacy notice')

- where we use personal data that has not been collected directly from the individual to communicate with them, we will provide the privacy notice, at the latest, when the first communication takes place;
 - if we plan to disclose personal data that has not been collected directly from the individual to another recipient, we will provide the privacy notice, at the latest, before the data are disclosed.
- 7.3. Each time the Council seeks to collect information from the individual, we must inform them why we need to process their personal information, including how we propose to use it, who we intend to share it with and the safeguards we have put in place.
- 7.4. Further information relating to the use of personal data may be viewed on our [Privacy Policy](#)
- 7.5. Further to this, the individuals also have the right to be informed of any significant data breach of their personal information. The reporting must be done without undue delay unless there are relevant reasons why they should not be informed, e.g. disclosure of the breach would cause them harm.

8. Right of access

- 8.1. [Article 15 UK GDPR](#) provides data subjects with the right to ask for confirmation that the Council processes or has processed data about them, copies of the personal data that the Council holds about them and other supplementary information, which includes:
- the purposes of the processing of the personal data;
 - the categories of the personal data being processed;
 - information about the recipients or categories of recipient to whom the personal data have been or will be disclosed;
 - confirmation of the period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
 - confirmation of their right to request rectification or erasure of personal data or restriction of processing of personal data concerning the individual or to object to such processing;
 - confirmation of their right to lodge a complaint with the ICO (see section 4.12);
 - confirmation of how to contact and make complaints directly to the Data Protection Officer;
 - provision of any information as to the source of the data, where it has not been collected from the data subject directly;

- confirmation as to whether any automated decision-making, including profiling, has taken place with their personal data and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for them;
- Confirmation of whether their personal data has been or will be transferred to a third country or to an international organisation, and if so, details of the appropriate safeguards put in place under the data protection legislation relating to the transfer.

8.2. The individual should provide the Council with as much detail as they can about the information they want to access. This will allow the Council to undertake precise searches, and locate the information at the earliest opportunity.

8.3. It is possible that should the Council need to contact the individual for further information to help locate the personal data they requested they may have to wait longer for a response.

9. Right to rectification

9.1. [Article 16 UK GDPR](#) provides individuals with the right to ask the Council:

- correct inaccurate information about them;
- update the information the Council holds, if it is incomplete

9.2. If the Council agrees that the personal information they have identified is factually inaccurate, it will be corrected.

9.3. If correction takes place, the Council will:

- endeavour to inform anyone with whom the Council may have shared the individual's personal data of any correction(s) the Council have made so they can rectify the information they hold about them;
- tell the individual who the recipients of their information are if they ask us to do this so the individual can check the recipient has updated the personal information they hold about them.

10. Right to object to processing

10.1. [Article 21 UK GDPR](#) provides Individuals with the right to object to the Council using their personal information where it is being processed for:

- direct marketing;
 - profiling whether linked to direct marketing or for other purposes
 - performing our statutory functions, tasks carried out in the public interest or when exercising official authority;
 - our legitimate interest or those of a third party;
 - scientific/historical research/statistics where:
 - this is likely to cause substantial damage or substantial or distress; or
 - involves decision-making about an individual
- 10.2. If they object to us using their personal information for direct marketing (or profiling linked to direct marketing) we will cease processing for this purpose(s) as soon as possible and no longer than 28 days after the individual has made the complaint.
- 10.3. The Council will only use personal data for direct marketing if the individuals have actively chosen to opt in to this service. If we intend to collect their personal data with the intention or expectation that we will send marketing material to them, we must tell them about this in advance and give them the chance to opt in to receiving such communications. If the individual has opted in and later decides that they no longer wish to receive marketing communications, we will not continue to hold their personal data for marketing purposes.
- 10.4. Where the individual makes an objection in relation to the processing of their personal information for public task/legitimate interests, this must be on grounds relating to their "particular situation". The Council must then cease the processing of the individual's personal data, unless:
- we can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the individual; or
 - the processing is for the purposes of the establishment, exercise or defence of legal claims.
- 10.5. If the individual objects to the use of their personal data for scientific/historical research or statistical purposes on one or both of the above grounds, we will carefully consider their request and let them know the outcome.
- 10.6. It may not always be possible to meet their objection if for example, the processing is carried out for the purpose of measures or decisions with respect to particular individuals where this is in accordance the law and is necessary for specified bodies to carry out approved medical research.

10.7. Where the individual objects to us processing their personal information for any of the other reasons above, we will:

- consider if we have compelling legitimate grounds for continued processing; and
- whether or not these grounds are sufficiently compelling to justify overriding the individuals privacy rights.

10.8. Where the law requires us to process their information to meet our statutory functions and public tasks, including our law enforcement functions, it is very likely that we will not be able to comply with the individuals request.

10.9. For example, individuals will not be able to use this right to prevent the Council from:

- taking measures to protect the health and safety of its staff;
- establishing, exercising or defending its legal rights;
- pursuing criminal investigations or proceedings.

11.10. National Data opt-out

10.10.1. The national data opt-out is a service that allows patients to opt out of their confidential patient information being used for research and planning.

10.10.2. The Council may collect health data in order to deliver specific services. The National Data Opt-out means that members of the public can decide that they do not want their information used for anything other than providing care or a direct service to them where the law does not specifically say it can be used in this way.

10.10.3. There are now rules in place concerning secondary use of health and social care data. This is when personal data is used for purposes not involving direct care, for example for research and planning purposes.

10.10.4. All health and care organisations are now required to respect these decisions and comply with the National Data Opt Out. The Council may not hold any data that the opt-out would apply to but needs to assess this on a case by case basis.

10.10.5. For further information; <https://digital.nhs.uk/services/national-data-opt-out>

11. Right to restriction of processing

11.1. [Article 18 UK GDPR](#) sets out the right to restriction of processing. This right may be exercised in circumstances where:

- we need time to consider the individuals representations where they are;
- contesting the accuracy of the personal information we hold about them; or
- objecting to our processing of their information (see previous right)
- it has already been determined the processing is 'unlawful' and they ask us to retain and 'restrict' its use;
- we no longer need to retain their personal information but they ask us to retain it for the establishment, exercise or defence of own legal claims.

11.2. If an individual makes a request we will let them know if we agree to restrict access to their information for one or more of the above reasons.

11.3. If we decide a restriction is appropriate, we will attempt to notify any recipients of their personal information of the restriction and let the individual know who they are if they ask us to do so.

11.4. Where processing is restricted, as well as storing the individual's personal information, we will only process it during the period of restriction:

- with their consent; or
- if it is necessary for the establishment, exercise or defence of legal claims;
- if it is necessary for the protection of the rights of another person; or
- if it is necessary for reasons of important public interest, including for example, communicating with the Information Commissioner.

11.5. Where a restriction is applied pending a determination of 'accuracy' or any 'objection' the individual may have submitted, we will let them know the outcome of their representations and will notify them prior to lifting the restriction.

11.6. Where the reason for the restriction is for one of the other reasons above, the erasure of the personal information will not take place until we have resolved evidential issues with the individual.

- 11.7. The Council must inform the individual if we decide to lift any restrictions placed on the processing of their data. They should receive this notification before we lift this restriction.
- 11.8. Where the Council puts a restriction on processing in place and has previously disclosed the data to others, we must inform each recipient of the restriction (unless this is impossible or would involve disproportionate effort).

12. Right to erasure ('right to be forgotten')

- 12.1. [Article 17 UK GDPR](#) provides individuals with a right to request that the Council erases their personal information in defined circumstances.
- 12.2. These defined circumstances are:
- if the Council is storing their personal information for longer than is necessary or in breach of a legal obligation that requires its erasure;
 - they decide to withdraw their consent and ask the Council to erase their personal information where there is no other legal ground for processing;
 - the Council has accepted an objection made by them to our processing of their personal information (see 11 above) and they have further requested that we erase the personal information in question;
 - the Council is processing or publishing their personal information without a legal basis for doing so;
 - where the Council is legally obliged to erase the information; or
 - the personal data was collected in relation to an offer of an information society service (in other words, for a fee over the internet) to a child.
- 12.3. The Council will carefully consider a request for erasure. Our response will outline whether or not we consider retention of their personal information is unwarranted.
- 12.4. The right of erasure or the "right to be forgotten" is not an absolute right. There are circumstances where it may not always be possible to agree to the individual's erasure request and we have listed a number of grounds below where it may be necessary for us to retain their information:
- in the interests of freedom of expression (special journalistic purposes)
 - in order to comply with a legal obligation;
 - for archiving in public interest;
 - for public health functions in public interest

- for exercising legal rights or defending legal claims
- 12.5. If we agree to erase their personal information, we will attempt to notify any recipients and let them know who they are if the individual ask us to do so (unless this is impossible or would involve disproportionate effort). If the Council has previously made their personal information public, we will also attempt to inform other data controllers who are processing the data that they have requested their erasure (although this will depend on the technical availability and cost of informing them of the request).

13. Right to data portability

- 13.1. [Article 20 UK GDPR](#) provides that, in certain circumstances, individuals have the right to request that the personal information they have supplied to an organisation be converted into a structured, commonly used and machine-readable format (e.g. a CSV file) so that it can be transmitted to another organisation.
- 13.2. This right is primarily intended to stimulate competition in the commercial sector by making it easier for consumers to switch from one supplier to another.
- 13.3. As most of the processing activities undertaken by the Council are governed by statute or as a result of legal obligations imposed on us, this right will only be engaged where:
- The individual has provided the personal information to us themselves, we are processing it on an automated basis, and the legal basis for our processing:
 - is based on their consent; or
 - is for entering into or the performance of a contract with them.
- 13.4. If they make a request for the personal information they have supplied to us to be converted into a portable format where our legal basis for processing falls within one of the grounds above, we will let them know our decision. We will be unlikely to agree to requests to transfer personal data that concerns other individuals, especially when providing the information will impact on the rights of those individuals or prejudice them in some way.
- 13.5. If we agree to their request, we will transfer the personal data in question directly to the other data controller they have identified, provided that such a transfer is technically feasible. However, we are not required to adopt or

maintain processing systems that are compatible with those of other data controllers.

14. Rights relating to automated decision making (ADM)

- 14.1. [Article 22 UK GDPR](#) sets out individual's rights in respect of automated decision making.
- 14.2. In general, decisions which effect the individual legally or have similarly significant effects are not permitted using solely automated processing (i.e. decision-making without human involvement), especially if this involves the use of 'Special Category Data'. This is because decisions made using automated electronic programmes or software do not involve human beings.
- 14.3. There are some exceptions where automated decision-making is permitted. This is where the processing:
 - is based on individuals explicit consent;
 - is necessary for entering into or the performance of a contract with them;
 - it is required or authorised by law
- 14.4. Where an automated decision is made about the individual based on one of the reasons above, they are entitled to be:
 - informed that our processing activity involves automated decision making and to be informed about the logic involved and the likely consequences of the processing for them;
 - told what measures and safeguards we have implemented to protect their privacy;
- 14.5. Where the Council undertakes automated decision making or profiling we will:
 - notify individuals about the processing;
 - provide a mechanism for them to request that we reconsider the decision or take a new decision that is not based solely on automated decision making;
 - carry out regular checks to ensure the automated decision making / profiling is working as intended.
- 14.6. We will only subject individuals Special Category Data to automated decision making or profiling where they have given explicit consent or where the processing is necessary for reasons of substantial public interest.

14.7. Within one month of receipt of the above notification, individuals have the right to:

- contest the automated decision; and
- ask that the automated decision be reconsidered by an appropriate person with the authority/seniority to reach a fresh decision that is not based solely on automated processing.

14.8. If they contest an automated decision and ask for it to be reconsidered, we will respond within the allowed time period and let them know whether or not this fresh decision has led to the same or a different outcome.

15. How individuals can exercise these rights

15.1. Individuals can exercise any of the data subject rights mentioned in this policy by writing to the Council's Information Governance Team directly at: information.governance@tameside.gov.uk, or informationanddata@tameside.gov.uk

15.2. Whilst individuals are encouraged to contact the Information Governance team directly, they can seek make their request to any person or service within the Council. Additionally their request can be made verbally as well as in writing and they do not have to specifically refer to the data protection legislation. For example subject access requests can often be made by data subjects who refer to the Freedom of Information Act 2000 in error – if the request is about their personal data, or made on behalf of another individual for that individual's personal data, it is still a subject access request even if they refer to FOIA 2000.

15.3. It is important that any employee who believes they have received an individual rights request contacts the information governance team as soon as possible for advice and/or for the request to be processed.

15.4. To help individuals understand how the Council processes their data in order to exercise any of their rights, we explain on our website how we collect and use personal information about them, including the types of information we process, what we will do with their information, who we may share it with, the 'lawful bases' (conditions) for processing it, and a list of our 'legal obligations' (powers) to use their personal data to provide services to you. They can view this page at <https://www.tameside.gov.uk/dataprotection/PrivacyNotice>

15.5. Further information in relation to submitting an individual rights request may

also be found via the following link:
<https://www.tameside.gov.uk/accesstoinformation>

- 15.6. For **all** requests, the Council will need evidence that that the requester is are who they say they are. This is for security reasons to ensure we are dealing with the individual and that none of their personal information is accessed or interfered with by anyone else falsely claiming to be them.
- 15.7. Individuals need to ensure they provide at least two forms of identification. Preferably a copy of a passport, driving licence, utility bill, council tax bill or bank statement bearing their full name and current postal address.
- 15.8. On receipt of their request, we will send them a written acknowledgement. In some circumstances we may also ask for additional information if necessary.
- 15.9. **Can someone else make a request for the individual?**
- 15.10. Individuals can ask anyone to act on their behalf. For example a friend, relative, solicitor or employee of a consumer organisation such as a Citizens Advice Bureau.
- 15.11. However, before we discuss or provide the individuals personal data to anyone acting on their behalf the individual must confirm to us in writing that they have their authority to do so. This will require the individual's signed authority, coupled with two forms of identification.
- 15.12. **What if a data subject 'lacks mental capacity'?**
- 15.13. A person with a lasting power of attorney appointed directly by the data subject or a Deputy appointed by the Court of Protection may exercise rights on behalf of the data subject.
- 15.14. **What about requests involving children?**
- 15.15. It is important to remember that personal data about a child, however young, is the child's personal data and is not the personal data of their parent or guardian.
- 15.16. A parent or guardian does not have an automatic right to personal data about their child and can only apply on the child's behalf if the child:
 - has given consent; or
 - is too young to have an understanding to make the application.

- 15.17. Unlike Scotland, there is no set age in England which recognises when children are automatically able to exercise data protection rights.
- 15.18. A child aged 13 or over is able to create an on line social media account without the consent of a person with parental responsibility.
- 15.19. As a general rule a child must have sufficient understanding and maturity to exercise their own rights and a common sense approach will be adopted in the event a child or young person submits a request.
- 15.20. For children aged under 13, it will generally be expected that a request is made by a person with parental responsibility. A 'best interest' consideration will be taken into account.
- 15.21. Individuals have the right to request that we erase personal data that was collected in relation to an offer of an 'information society service' to a child (see section 3.4).

15.22. **How do individuals evidence parental responsibility?**

- 15.23. The following evidences may be accepted as proof of parental responsibility:

- Birth Certificate
- Court Order
- Adoption Record
- Special Guardianship Order

15.24. **When can individuals expect a response?**

- 15.25. We aim to respond to requests without undue delay and no later than one calendar month counted from the first working day after we are in receipt of an individual's request, and:

- proof of their identity, **and**
- any further information (where we have requested this from them) we need to process their request and/or locate and retrieve their personal information.

- 15.26. Where it is not possible to respond sooner and the last day before expiry of one calendar month, falls over a weekend or on a bank holiday, the latest due date will be treated as the first working day after the weekend or bank holiday.

15.27. If a request is complex, we may need to extend the length of time required to respond.

15.28. If this applies, we will let the individual know before the latest due date on which they would be expecting to hear back from us.

15.29. Data protection legislation says we can extend the length of time to respond by a maximum of a further two calendar months.

15.30. Where it is not possible to respond sooner and the last day before expiry of the second calendar month, falls over a weekend or on a bank holiday, the latest due date will be treated as the first working day after the weekend or bank holiday.

15.31. We will always try to respond as quickly as we can.

15.32. **What will we send the individual when we respond?**

15.33. At the time of fulfilling the request, alongside copies of any information about the individual which they have requested and we are able to disclose, we will also provide the following information:

- the reasons why it is necessary to process their personal information;
- the types of personal information we process;
- the recipients or categories of recipient to whom their personal information have been or will be disclosed, including any recipients in third countries or international organisations and if relevant, the safeguards applicable to the transfer;
- where possible, the envisaged period for which their personal information will be stored, or, if not possible, the criteria used to determine that period;
- the right to request rectification, erasure of personal information or to object or seek to restrict such processing;
- the right to lodge a complaint with a supervisory authority (see section 4.12);
- the source(s) of any personal information we hold that has not been collected directly from them;
- whether or not decisions are made about the individual solely using automated means, including profiling, without human intervention and, if so, provide meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for you.

15.34. Will individuals have to pay a charge?

15.35. Ordinarily we will not charge a fee for fulfilling a request from the individual.

15.36. The only exception is where the individual makes repeat requests for the same or similar information. In these cases, we reserve the right to charge a reasonable fee based on the administrative costs of supplying further copies if we consider a reasonable time period has not intervened since fulfilling a previous request.

15.37. Where the right of data portability is engaged, we must also provide information through this route free of charge (see section 3.7).

15.38. Will individuals get all of the information they are requesting?

15.39. This is likely to be the case.

15.40. But it is important to note that the right of access to their own information does not extend to information about other people who may be identified in the information that also refers to them.

15.41. The Council may therefore redact (blank out) personal information about other individuals (called 'third parties' in the data protection laws) where we are satisfied it is reasonable in the circumstances to do so. We may withhold or redact some information the individuals request about themselves where it is possible to identify a third party.

15.42. In some cases information may be so interlinked that it is not possible to fulfil their request without breaching another person's privacy rights.

15.43. The names of professional staff (whether directly employed by us or not) involved in decision-making about the individuals care and education will often be disclosable and their identities will not be automatically redacted, unless this is warranted in a particular case.

15.44. The law recognises that there are occasions when it may be appropriate to withhold certain information and provide exemptions in specified circumstances. For example, it may be exempt if providing it to the individual would compromise the prevention or detection of crime or the prosecution of offenders. In certain cases, we may also withhold some information relating to education, health and social work.

15.45. If we withhold information on the basis that it is exempt from disclosure, where it is possible to do so, we will explain the exemption(s) we are relying on and the reasons why one or more are necessary.

15.46. Can individuals choose the format in which their information is supplied?

15.47. Once we have located individual's personal data we will provide copies to them in the same format they first contacted us, unless specified otherwise.

15.48. Where individuals have submitted their request electronically or asked us to respond in a particular format, we will try to do so wherever this is reasonably practicable.

15.49. Can The Council refuse requests?

15.50. In certain circumstances we may refuse to act on individuals request if we consider that their request is unfounded, excessive or repetitive in nature.

15.51. We will give our reasons if we refuse to comply with requests on any of these grounds.

15.52. What if individuals am not satisfied with our response or it is taking too long?

15.53. Upon receipt of individual's requests we have one calendar month to provide them with a response, or contact them to tell them how much longer we need to fulfil their request.

15.54. The Information Commissioner's Office (ICO) is the UK's independent regulator responsible for upholding and enforcing the rights of individuals under the data protection laws.

15.55. If individuals do not hear from us by the latest due date or are not satisfied with the response they have been given, they have the right to complain to the ICO.

15.56. If individuals consider that personal information we hold about them is incomplete and we do not agree with this, we may offer them the option of adding a supplementary statement explaining why they consider the information we hold is incomplete.

15.57. If we disagree with their view that the information we hold about them is factually wrong, or refuse their request for erasure, then in our response we

will explain the basis for our decision and give them details about their right to complain to the ICO if they are not satisfied.

They can contact the ICO

Via their website: <https://ico.org.uk/make-a-complaint/>.

By post:
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

16. Training

- 16.1. The Council will provide relevant training both on line and face to face to ensure that staff understand the legislation and its application to their role.
- 16.2. 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.
- 16.3. Completion of training will be monitored by the Information Governance Team and all employees must have regard to the 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.

17. Time scales and escalation

Individual Right	Absolute	Action	Statutory Time Scale	Escalation
The Right to be Informed	Yes	Provide Privacy Notice at the point of data collection wherever possible	ASAP	Information Governance Team, then DPO, Head of Service

The Right of Access	Yes	Collate, redact and provide in an agreed format. Explain grounds for redactions	One calendar month unless deemed complex [add 2 months]. Clock start when ID documents have been received.	Information Governance Team, then DPO, Head of Service
Right to rectification	Yes	Amend record to be accurate and up to date	ASAP but no longer than 1 calendar month	Information Governance Team, then DPO, Head of Service
Right to erasure	No	Remove all records if lawful, there needs to be a compelling reason to continue to process Unlikely this will be upheld in public sector.	ASAP but no longer than 1 calendar month	Information Governance Team, then DPO, Head of Service
Right to restrict processing	No	There are some circumstances where a data subject can request restrictions	ASAP but no longer than 1 calendar month	Information Governance Team, then DPO, Head of Service
Right to data portability	No	Data subjects have a right to a copy of their data in machine readable format to transfer to a new data controller	ASAP but no longer than 1 calendar month	Information Governance Team, then DPO, Head of Service
Right to object to processing	No	There are conditions where this may be upheld :direct marketing, research & Stats	ASAP but no longer than 1 calendar month	Information Governance Team, then DPO, Head of Service

Rights in relation to automated decision making	Yes	Data Subjects can request human intervention, express their views and obtain an explanation.	ASAP but no longer than 1 calendar month	Information Governance Team, then DPO, Head of Service

18. Compliance and Monitoring

- 18.1. 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 at information.governance@tameside.gov.uk or informationanddata@tameside.gov.uk.
- 18.2. 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.
- 18.3. This policy will be reviewed regularly by the Information Governance Team to ensure that it is updated in line with any change in legislation. This will happen annually unless there are any major changes
- 18.4. The Council will continue to review this effectiveness of this policy to ensure that it is achieving its intended purpose.

19. CONTACT DETAILS

Data Protection Officer; Head of Information Governance
 TMBC, Tameside One, Market Place, Ashton-under-Lyne, Tameside
 Email: information.governance@tameside.gov.uk

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

Information Commissioner
 Information Commissioners Office, Wycliffe House, Water Lane, Wilmslow,
 Cheshire SK9 5AF
 Tel: 0303 123 1113
www.ico.org.uk

APPENDIX 1: Definitions

- "Personal information" means any information relating to an identified or identifiable living person. An identifiable person is anyone who can be identified, directly or indirectly, by reference to an identifier, such as a name, identification number or online identifier.
- "Special or Sensitive Personal information" is information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and personal information relating to criminal offences and convictions.
- "Processing" means any activity that involves the use of personal information. It includes obtaining, recording or holding the information, or carrying out any operation or set of operations on the information including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal information to other Recipients.
- "Data Subject" a living, identified or identifiable individual about whom we as the Controller hold personal information.
- "Controller" means the person or organisation (in this case us) that determines when, why and how to process personal information.
- "Privacy Notices" are notices setting out the information given to you at the time we collect information from you or within a reasonable time period after we obtain information about you from someone else. These notices may take the form of an overarching privacy statement (as available on our web site) or apply to a specific group of individuals (for example, service specific or employee privacy notices) or they may be stand-alone, one time privacy statements covering processing related to a specific purpose.
- "Consent" must be freely given, specific, informed and unambiguous indication of an individuals' wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- "Explicit Consent" requires a very clear and specific statement, leaving no room for misinterpretation.

- "Third Party" is a living individual other than the person who is the data subject
- "Recipient" means a person or organisation who receives your personal information from us. This may be a company with whom we have entered into a contract to provide services on our behalf or another Controller with whom we are either required or permitted to share personal information.
- "Latest due date" means one calendar month counted from the first working day after proof of ID and any requested information is received by us, except where this falls on a weekend or a bank holiday in which case the "latest due date" is treated as the first working day after the weekend or bank holiday. The same method is applied to calculating the "latest due date" for complex requests where an extension of time is permitted and claimed.
- "Automated Processing" means any processing of personal information that is automated through the use of computers and computer software.
- "Automated Decision-Making (ADM)" means a decision which is based solely on Automated Processing (including Profiling) which produces legal effects or significantly affects an individual. Data protection legislation generally prohibits Automated Decision-Making except in defined circumstances, subject to certain conditions and safeguards being met.
- "Profiling" means the recording and analysis of a person's psychological and behavioural characteristics, so as to assess or predict their capabilities in a certain sphere or to assist in identifying categories of people.
- "Data protection legislation" has the same meaning as defined in the Data Protection Act 2018, and includes GDPR, the Data Protection Act 2018 and any regulations or secondary legislation made underneath them.
- "General Data Protection Regulation (GDPR)" means the General Information Protection Regulation ((EU) 2016/679).

APPENDIX 2: Related Policies and Procedures

- Data Protection Policy
- Data Sharing Policy
- Data Quality Policy
- Information Asset Management Policy
- Records Management Policy
- Records Retention and Disposal Policy

- Records Retention Schedule
- Individual Rights Policy
- Disciplinary Policy
- Employee Code of Conduct
- Freedom of Information Act (FOI) and Environmental Information Regulations (EIR) Policy

APPENDIX 3: Legislative Framework

The Anonymisation and Pseudonymisation Policy is set in the context of the following legislation and guidance:

- [UK General Data Protection Regulation 2018](#) and [Data Protection Act 2018](#) – that requires that personal information must be handled and stored in a confidential manner
- [The Human Rights Act 2000](#) - everyone has the right to respect for their private and family life, home and correspondence.
- [Freedom of Information Act 2000](#) and [Environmental Information Regulations 2004](#) - Public authorities, if requested, must disclose information that they hold.
- [Localism Act 2011](#) - Highlights the importance of transparency and accountability of public bodies and raw data.
- [Local Government Transparency Code](#) - All local authorities must publish the datasets required by the code, in some cases in prescribed formats [The Re-use of Public Sector Information Regulations 2015](#) (PSI) Encourages the reuse of public sector information by third parties for purposes other than the initial public task it was produced for. The Regulations govern what and how information has to be made available for re-use.

Online Resources

- ICO – <https://ico.org.uk/>
- TMBC intranet