Pseudonymisation and Anonymisation Policy

Author: Rachel Everitt

Date: September 2024

Version: v0.1

Title	Pseudonymisation and Anonymisation
Author	Rachel Everitt
Owner	Data Protection Officer
Created	September 2024
Approved by	Audit Committee
Date of Approval	February 2025
Review Date	February 2027

Document Version Control

Document Version Control	
Issue Number	
0.01	October 2024

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 It supersedes any previous versions of this document, which are now withdrawn.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

Bury Council works collaboratively with other public sector organisations, voluntary organisations and private enterprises to drive beneficial outcomes for the Bury area.

In order to fulfil its functions, 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.

As a public authority, Bury Council is required to comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. Both of these pieces of legislation require Bury Council to process only the minimum amount of personal data needed for one or more specified purpose. The council is also required to not use information that identifies individuals unless necessary.

The UK GDPR provides a set of principles that the council must follow to handle personal data appropriately and in accordance with the law. The principle that supports the practice of only using the amount of personal data necessary is called the Data minimisation principle' and is set out in Article 5(c) of GDPR. Data minimisation is also formally recognised in the third Caldicott principle in relation to processing patient data and information and it states: 'Don't use personal confidential data unless it is absolutely necessary'.

There are various ways in which data can be minimised, where personal fata isn't necessary for the purposes or the outcomes that are trying to be achieved, and so pseudonymisation and/or anonymisation techniques should be applied to the data.

Effective pseudonymisation and/or anonymisation processes depend upon robust information governance and effectively trained staff who understand the importance of data protection and confidentiality.

Anonymisation is the process of removing, replacing and/or altering any identifiable information that can point to the person(s) it relates to.

Pseudonymisation is the technical process of replacing the identifying information to protect the individual's identity whilst allowing the recipients to link different pieces of information together.

This policy sets out the commitment of Bury Council to comply with the data minimisation principle and the use of pseudonymisation and anonymisation.

This policy is part of Bury Council's Information Governance Framework and should be read in conjunction with the other policies and procedures within the framework.

Scope

This policy applies to all personal information including health data, special category/criminal conviction data used, stored or shared by or with Bury Council whether in paper or electronic form.

The policy applies to all Bury Council employees, seconded staff members, temporary staff, councillors, volunteer and third-party contractors.

This policy applies to data processing where Bury Council is the data controller in its own right or is a data controller in relation to multi-agency data sharing partnership.

2. Policy

This policy states how Bury Council will comply with the GDPR's data minimisation principle using anonymisation and pseudonymisation techniques.

Data protection legislation classes pseudonymised data as personal data and therefore must be processed in accordance with all data protection legislation. If Bury Council has access to pseudonymised data and the identifiable personal confidential data.

Data protection legislation states that data which is truly anonymised in such a way that individuals cannot be identified or re identified does not fall within the scope of the UK GDPR and therefore does not fall within the scope of the Data Protection Act either.

It is always preferable to fully anonymise any data that has the potential to reveal something personal about an individual, either from that data alone or when combined with other data.

Where data cannot be used in an anonymised format, due to the need to link datasets, because data may ultimately need to be re-identified or processed in identifiable format, the personal or data or pseudonymised data may be used provided there are strict controls in place to prevent unauthorised access and unauthorised re-identification.

The key advantages of using anonymised data as opposed to identifiable data include:

- it is easier to use anonymised data in new and different ways because the data protection legislation "purpose limitation rules do not apply;
- protection against unauthorised access or disclosure of personal data; fewer legal restrictions apply;
- allow for the sharing of data with colleagues and teams for analysis
- allows organisations to make information public while still complying with their data protection obligations; and
- the disclosure of anonymised data is not a disclosure of personal data.

Bury Council will carry out a thorough risk analysis on the likelihood and potential consequences of re-identification at the initial stage of producing and disclosing anonymised or pseudonymised data. The GMCA will always use a

DPIA (Data Protection Impact Assessment) to undertake this assessment of risk, in line with Article 35 of GDPR.

The risk of re-identification will differ according to the way the anonymised or pseudonymised information is disclosed, shared or published. Publication to the wider public would be considered far more risky than limited access.

Any pseudonymization and anonymisation techniques used in projects undertaken by Bury Council must therefore be employed as part of a 'holistic methodology' of technical and non- technical processes to protect personal data enshrined in the concept of privacy by design and default (Article 25).

Anonymisation

Bury Council will use de-identification and anonymisation techniques to obscure or remove the identifiable data items within a person's records sufficiently that the risk of potential identification of the subject or a person's record is minimised to acceptable levels, so as to provide effective anonymisation, where appropriate. Recital 26 of GDPR defines anonymous information, as "…information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable". The GDPR does not apply to anonymised information as set out above in Section 6.

Anonymised data will allow information which originated as personal confidential data to be available in a form that is rich and usable, whilst protecting the confidentiality of the individual.

The Council will continue to comply with role-based access controls when using de-identified and anonymised data.

The organisation will achieve de-identification and anonymisation by:

- Removing personal identifiers (e.g. name, date of birth, physical description etc)
- The use of identifier ranges, for example; value ranges instead of age

- Aggregation
- Using a pseudonym (although, as covered further below, pseudonymising data will not necessarily completely ensure that re-identification is impossible)

The organisation will ensure that any commissioning and contracting on behalf of Bury Council will include assurances that the Provider's processes are robust in respect of the supply of data and data minimization principles.

The most up to date guidance from the Information Commissioners Office on Anonymisation can be viewed here;
https://ico.org.uk/media/1061/anonymisation- code.pdf

Pseudonymisation

Pseudonymisation is the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable human being. Essentially this means substituting the identifiable part of the data with something else, in a way that the data can only be re-identified using a key for example.

Bury Council will effectively pseudonymise data by:

- Removing personal identifiers and ensuring Personal Identifiable Data is replaced with a unique pseudonym
- When using pseudonymisation externally, it's important to use different pseudonyms internally, such that internal data use/processes are not compromised
- Pseudonymised data will have the same security applied to it as all other Personal Identifiable Data.

3. Compliance and Monitoring

Legal and Professional Obligations

Bury Council will take actions to comply with the relevant legal and professional obligations, in particular:

- General Data Protection Regulation and Data Protection Act 2018
- Human Rights Act 1998
- Common Law Duty of Confidentiality
- The Information Commissioner's Office (ICO) code: anonymisation: managing data protection risk code of practice
- NHS Digital Data Security and Protection Toolkit

Training

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

All staff must complete mandatory data protection training every year and undertake any further training provided by Bury Council to enable them to perform their duties appropriately specifically those staff responding to complaints, Subject Access Requests and Freedom of Information requests.

Completion of training will be monitored by the Policy and Compliance 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.

If an employee is in any doubt about how to handle personal information or how to apply the pseudonymisation/anonymisation techniques mentioned above, they should speak to their line manager or contact the Policy and Compliance Team by emailing IG@bury.gov.uk.

Policy Review

This policy will be reviewed regularly by the Policy and Compliance Team to ensure that it is updated in line with any change in legislation.

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

Any breaches of the principles in this policy must be reported to the information governance team immediately; ig@bury.gov.uk.

Where staff fail to follow and comply with this policy it may result in disciplinary action via the HR channels.

4. Policy exemption

Occasionally there may be situations where exceptions to this policy are required, as full adherence may not be practical, could delay business critical initiatives or could increase costs.

Where the significance and purpose of the data does not justify a particular aspect (for example the cost of building an internal system validation check outweighs the benefit of the additional data accuracy) then this should be risk assessed on a case-by-case basis. Where there are justifiable reasons, the Data Protection Officer must be consulted immediately using ig@bury.gov.uk.