Tollesbury School

Minimisation of Personal Data Procedure

Title	Minimisation of Personal Data
Date Approved	20th September 2018
Approved by	Full Board of Governors
Review Date	September 2021

Contents

1. Introduction 3
2. Policy References 3
3. Data Minimisation Procedure 3
3.1. Obtaining Minimal Personal Data 3
3.2. Removing Personal Data (Anonymising & Pseudonymising) 4
4. Advice and Support 7
5. Breach Statement 8

1. Introduction

2. Policy References

2.1. This procedure is a requirement of the following policies:

- Data Protection Policy

3. Data Minimisation Procedure

3.1. Obtaining Minimal Personal Data

3.1.1. Legal Requirement

Data Protection law requires all Organisations to ensure that the personal data they obtain and process is limited to the minimal amount required to effectively achieve the purpose for which it was obtained:

Personal data shall be: "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed"

General Data Protection Regulations 2016, Article 5(c)

3.1.2. Privacy by Design

In order to comply with the requirement of Principle 5(c), and to be able to evidence to the Regulator that compliance is embedded within the privacy culture of the organisation, the following measures must be in place:

3.1.2.1. Record of Processing Activity

- All flows of personal data into the Organisation must be identified on the Data Lifecycle Mapping element of our Record of Processing Activity.
- From this data, we can ensure we identify all instances where personal data is obtained
- From this basis we can ensure that all methods of collecting personal information from Data Subjects are reviewed to ensure that they are provided with or linked to a Privacy Notice which includes detail compliant with the law.

3.1.2.2. Data Collection

- The Data Collection forms (i.e. the means by which the Data Subject provides personal data to us) must be reviewed to ensure they gather only information that is relevant to the stated purposes

- Forms must actively limit the scope for Data Subjects to provide additional superfluous personal data, making good use of tick boxes, clearly worded text boxes specifying what data is required, and avoiding the use of 'free-text' boxes where narrative responses invite uncontrolled provision of data.
- Forms should avoid requesting 'desirable' or 'nice-to-have' data as by definition this is not 'necessary' to fulfil the stated purposes.

3.1.2.3. Privacy/ Data Protection Impact Assessments

- All activities which obtain personal data must be reviewed to assess whether an Impact Assessment is required to fully consider the legality of the processing of personal data under Data Protection law
- The Privacy Impact Assessment (and the Data Protection Impact Assessment for 'high risk' processing) require an Owner to confirm that an accurate Privacy Notice is in place and that the Principle under Article 5(c) is being met. This means the organisation is satisfied that the activity:
    - Clearly explains what the purpose of obtaining the data is for
    - We obtain only the data that is necessary to fulfil that purpose
- The approved Assessment(s) for new activities and reviews of existing and future activities will provide evidence to the regulator that the organisation has a comprehensive procedure for ensuring that only minimal personal data is being processed.

3.2. Removing Personal Data (Anonymising & Pseudonymising)

3.2.1. Legal Requirement

The use of anonymisation and pseudonymisation can further support the requirement under Article 5(c) by allowing the processing of data having removed the personally identifiable elements yet retaining associated data to undertake useful research/ analysis.

3.2.2. Terms:

Anonymisation: is the removal of information that could lead to an individual being identified, either on the basis of

a) the removed information or
b) the removed information combined with other information held.

Pseudonymisation: is a procedure by which the fields most likely to identify an individual within a data record are replaced by one or more artificial identifiers, or pseudonyms. There can be a single pseudonym for a collection of replaced fields or a pseudonym per replaced field. The use of pseudonyms allows us to hold the original dataset to re-identify the data at a later date if it is necessary.

3.2.3. Is Anonymised/ Pseudonymised data Personal Data?

There is a clear view that where an organisation converts personal data into an anonymised form and discloses it, this will not be considered a disclosure of personal data. This means that Data Protection Act law no longer applies to the disclosed data, therefore:

a) there is an obvious incentive for organisations that want to publish data to do so in an anonymised form;
b) it provides an incentive for researchers and others to use anonymised data as an alternative to personal data wherever this is possible; and
c) individuals' identities are protected

It is important to note however, that the originating organisation must comply with Data Protection law as they are in possession of the original personal identifiable dataset; and therefore are able to re-identify the data. This means that the originating organisation is processing personal data, even if that data has been anonymised. If the recipients do not have access to the original data, or some other linkable data, they are not processing personal data and the originating organisation has not disclosed it.

3.2.4. How do I Pseudonymised/ Anonymise Personal Data safely?

We will comply with the Health & Social Care Anonymisation Standard and its associated guidance to ensure that the privacy of individuals is upheld.

3.2.5. Is Consent required?

No. Data Protection law provides various 'conditions' for legitimising the processing of personal data, including its anonymisation/ pseudonymisation. Consent is just one condition, and the law usually provides alternatives. Where data has been effectively anonymised/ pseudonymised it does not constitute personal data and therefore a condition for processing is not required.

The DPA only gives the individual a right to prevent the processing of their personal data where this would be likely to cause unwarranted damage or distress. In the Information Commissioner's Office's view, provided there is no likelihood of anonymisation/ pseudonymisation causing unwarranted damage or distress, as will be the case if it is done effectively, then there will be no need to obtain consent as a means of legitimising the processing.

3.2.6. Informing the Data Subjects

When using personal data for research purposes, the data can be anonymised to avoid the identification of an individual, or if consent has been given then the data can remain identifiable.

We will need to check the relevant privacy notice which explains how they data would be processed to ensure that it correctly advised individuals appropriately that their personal data may be used for research. For example, if a privacy notice advises that we use data for 'service improvement' as a specified purpose you will be able to use personal data for this purpose. Similarly, if you intend to anonymise data for research, you should state in your privacy notice that anonymised data will be used for research purposes.

3.2.7. Retention

As explained above, the data is no longer viewed as Personal Data therefore the principle to retain no longer than necessary in Data Protection law is not engaged.

3.2.8. Publishing Pseudonymised/ Anonymised Datasets

It is important to draw a clear distinction between:

- Publication to the world at large, e.g. under the Freedom of Information Act 2000, or open data. Here there is no restriction on the further disclosure or use of the data and no guarantee that it will be kept secure; and

- Limited access, e.g. within a closed community of researchers. Here it is possible to restrict the further disclosure or use of the data and its security can be guaranteed. The advantage of this is that re-identification and other risks are more controllable, and potentially more data can be disclosed without having to deal with the problems that publication can cause

Limited access is particularly appropriate for the handling of anonymised data derived from sensitive source material or where there is a significant risk of re-identification.

Once data has been published under a licence, such as the Open Government Licence, it may be impossible to protect it from further use or disclosure or to keep it secure. However, the Open Government Licence does make it clear that while anonymised data falls within the scope of the licence, users and re-users are not permitted to use the data in a way that enables re-identification to take place. However, this may be difficult or impossible to enforce.

3.2.9. Trusted Third Parties

A trusted third party (TTP) arrangement can be particularly effective where a number of organisations each want to anonymise the personal data they hold for use in a

collaborative project. This model is being used increasingly to facilitate large scale research using data collected by a number of organisations.

Typically, the TTP will operate a data repository to which the various participating organisations will disclose their personal data, or alternatively pseudonymise their data at source before providing to the TTP. Where necessary a TTP can be used to convert personal data into an anonymised form. This is particularly useful in the context of research, as it allows researchers to use anonymised data in situations where using raw personal data is not necessary or appropriate. TTPs can be used to link datasets from separate organisations, and then create anonymised records for researchers.

A TTP analyses the data to match the records of individuals who appear in both datasets. A new dataset can be created which contains research data without identifying individuals. The researchers have access to useful data, in an environment which prevents them identifying individual subjects.

The personal data can then be anonymised in 'safe', high security conditions and to an agreed specification, allowing the subsequent linkage of anonymised individual-level data, for example.

The great advantage of a TTP arrangement is that it allows social science research to take place, e.g. using anonymised data derived from health and criminal justice records, without the organisations involved ever having access to each other's personal data. Security, anonymisation and anti-re-identification measures taken by the TTP should be covered in an agreement.

3.2.10. Further Guidance

www.ico.org.uk
Anonymisation Code of Practice – November 2012
HSCIC Anonymisation Standard
HSCIC Anonymisation Guidance

4. Advice and Support

4.1. If you have any issues over the clarity of these procedures, how they should be applied in practice, require advice about exemptions from the requirements or have any suggestions for amendments, please contact Headteacher/Senior Leadership Team or ECC DPO Lauri Almond DPO@essex.gov.uk

5. Breach Statement

5.1. A breach of this procedure is a breach of Information Policy. Breaches will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.