Processing Special Categories of Personal Data Policy

Policy document in respect of personal data processing (the appropriate policy document)

This is the “appropriate policy document” for Bury Council that sets out how we will safeguard personal data that:

- is categorised as special and/or relates to criminal convictions or offences in respect of our general processing activities,
- is categorised as sensitive and processed by us in our capacity as a ‘competent authority’ for law enforcement functions

It meets the requirements specified in Data Protection Act 2018 (DPA 2018), that an appropriate policy document be in place where our processing of personal data is necessary and falls within one of the above categories.

The Table below summarises the relevant DPA 2018 provision stipulating this policy requirement and the types of processing to which this applies.

General processing	
Schedule 1, Part 1 Paragraph 1(b) & Part 4	Processing of SCD for employment, social security or social protection *(as described in paragraph 1 of Schedule 1)*
Schedule 1, Part 2, paragraph 5 & Part 4	Processing of SCD in the substantial public interest *(as described in paragraphs 6 – 28 of Schedule 1)*
Schedule 1, Part 3 & Part 4	Processing relating to criminal convictions and offences *(as described in paragraphs 29 – 37 of Schedule 1)*
Law Enforcement	
Part 3, Section 35(2)(a); & Schedule 8	Processing of sensitive personal data by ‘competent authorities' *(as described in paragraphs 1 – 9)*

Procedures for securing compliance

Article 5 of the General Data Protection Regulation (GDPR) sets out the data protection principles for general processing. Our procedures for ensuring that we comply with these principles are set out below.

Principle 1 Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.	• that personal data is only processed where a lawful basis applies, and where processing is otherwise lawful • we only process personal data fairly, and ensure that data subjects are not misled about the purposes of any processing • that data subjects receive full privacy information so that any processing of personal data is transparent *(see qualification in context of law enforcement functions below)*
Principle 2 Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.	• we only collect personal data for specified, explicit and legitimate purposes, and we inform data subjects what those purposes are in a privacy notice • we do 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
Principle 3 Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed	• we only collect the minimum personal data that we need for the purpose for which it is obtained • we ensure that the data we collect is adequate and relevant
Principle 4 Personal data shall be accurate and, where necessary, kept up to date	• we keep personal data accurate and up to date where necessary • we take particular care to do this where our use of the personal data has a significant impact on individuals
Principle 5 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.	• we only keep personal data in identifiable form 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 is deleted or rendered permanently anonymous
Principle 6 Personal data shall be processed in a manner that ensures appropriate security of the	• we ensure that appropriate organisational and technical measures are in place to protect personal data

personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.	• we ensure equivalent measures apply throughout our supply chains

The data protection principles in respect of processing by competent authorities for law enforcement functions are set out in paragraphs 35 – 40, Chapter 2 of Part 3 of the DPA 2018. These principles have largely the same effect as above. However, the main area of difference relates to the first principle for law enforcement which omits the transparency obligation as it is recognised circumstances may apply where this could be prejudicial to effective law enforcement.

Accountability principle

As an accountable and responsible controller for the personal data we process, we must be able to demonstrate compliance with these principles. Our Senior Information Risk Owner is responsible for ensuring that Bury Council is compliant with these principles.

We 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
- ensure that we designate a Data Protection Officer to provide independent advice and monitoring of our personal data handling, and that this person has access to report to the highest management level of Bury Council
- 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 legislation
- notify any security failure that leads to a serious personal data breach presenting a high risk to the privacy rights of individuals in line with data protection legislative requirements.

Our policies as regards retention and erasure of personal data

We will ensure, where personal data is categorised as special, relates to criminal convictions or offences or is sensitive personal data processed for law enforcement functions, that:

- there is a record of that processing, 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 the personal data for the purpose for which it was obtained, we will delete it or render it permanently anonymous
- data subjects receive full privacy information about how their data will be handled and that this includes our processing for law enforcement purposes, where it is possible to do so,

- privacy information includes the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period

Further information

For further information about our compliance with data protection legislation, please contact us:

Data Protection Officer, Bury Council, Town Hall, Knowsley Street, Bury BL9 0SW

Review

This policy will be reviewed on an annual basis or earlier in the event new legislation or guidance comes into force.