Wombridge Primary School

Data Protection Policy

Date: February 2019
Review: February 2020

1. Introduction

The General Data Protection Regulations (GDPR) defines UK law on the processing of data on identifiable living people. It is the main piece of legislation that governs the protection of personal data in the UK. Personal information is information about a living individual, who can be identified from the information.

1.1 Telford & Wrekin Council is committed to protecting the privacy of individuals and handles all personal information in a manner that complies with the GDPR. It is the **personal responsibility** of all employees (temporary or permanent), Members, contractors, agents and anyone else processing information on our behalf to comply with this policy.

1.2 Any deliberate breach of this policy could amount to a criminal offence under one or more pieces of legislation, for example the Computer Misuse Act 1990 and the GDPR. All breaches will be investigated and appropriate action taken.

1.3 This policy explains what the Council's expectations are when processing personal information and should be read in conjunction with the Corporate Information Security Policy (CISP).

2. GDPR Principles

2.1. The GDPR is supported by a set of 6 principles which must be adhered to whenever personal information is processed. Processing includes obtaining, recording, using, holding, disclosing and deleting personal information.

2.2 The GDPR principles state that personal information must:

Be processed fairly, lawfully and transparently	**Obtained for a specified, explicit and legitimate purpose**	**Be adequate, relevant and limited to what is necessary**
Be accurate and where necessary up to date	Not be kept longer than is necessary	Be handled ensuring appropriate security

3. Access and Use of Personal Information

3.1 Access and use of personal information held by the Council, is only permitted by employees (temporary or permanent), Members, contractors, agents and anyone else processing information on our behalf, for the purpose of carrying out their official duties. Use or access for any other purpose is not allowed. Deliberate unauthorised use and access to copying, destruction or alteration of or interference with any personal information is strictly forbidden.

4. Collecting Personal Information

4.1. When personal information is collected, for example on a questionnaire, survey or an application form, the 'data subject' (that is the person who the information is about) must be told. This is known as a Privacy Notice. Guidance on what information needs to be included in a Privacy Notice can be found on the GDPR intranet page.

4.2 Personal information collected, must be adequate, relevant and not excessive for the purpose of the collection. A person's name and other identifying information should not be collected where anonymous information would suffice.

4.3 If the information is collected for one purpose, it cannot then be used for a different and unconnected purpose without the data subject's consent unless there is another lawful basis for using the information (see section 5 below). It must be made clear to the 'data subject' all the purposes that their information may be used for **at the time the information is collected**.

5. Lawful Basis for Processing

5.1 When Telford & Wrekin Council processes personal information, it must have a lawful basis for doing so. GDPR provides a list of 'conditions' when we can process personal or 'special category' personal information. This is contained within Article 6 and Article 9 of the regulations ***(see Appendix 1)***.

5.2 The GDPR defines special category personal information as information relating to:

- Race and ethnic origin
- political opinion
- religious or philosophical beliefs
- trade union membership
- processing of genetic/biometric data to uniquely identifying a person
- physical or mental health or medical condition;
- sexual life

5.3 Whenever the Council processes personal information, it must be able to satisfy at least one of the conditions in Article 6 of the GDPR and when it processes 'special category' personal information; it must be able to satisfy at least one of the conditions in Article 9 of the GDPR as well.

5.4 The Council can process personal information if it has the data subject's consent (this needs to be 'explicit' when it processes sensitive personal information). In order for consent to be valid it must be 'fully informed' which means the person giving consent must understand what they are consenting to and what the consequences are if they give or refuse consent. Consent must not be obtained through coercion or under duress and should be recorded. Guidance on how consent should be managed can be found on the GDPR intranet page.

6. Disclosing Personal Information

6.1 Personal information must not be given to anyone internally or externally, unless the person giving the information is fully satisfied that the enquirer or recipient is authorised in all respects and is legally entitled to the information.

6.2 If personal information is given to another organisation or person outside of the Council, the disclosing person must identify the lawful basis for the disclosure (see section 4 above) and record their reasoning for using this basis. This record as a minimum should include;

- a description of the information given;
- the name of the person and organisation the information was given to;
- the date;
- the reason for the information being given; and
- the lawful basis.

6.3 If an information sharing agreement or protocol exists, this should be adhered to when providing personal information to others. The agreement/protocol will provide the legal basis for disclosure.

6.4 In response to any lawful request, only the minimum amount of personal information should be given. The person giving the information should make sure that the information is adequate for the purpose, relevant and not excessive.

6.5 When personal information is given either externally or internally, it must be communicated in a secure manner. For external communications use GCSX or the Secure Communications System (SCS), special delivery or courier, etc. For internal communications either hand deliver or make sure you email the information to the correct recipient.

7. Accuracy and Relevance

7.1. It is the responsibility of those who receive personal information to make sure so far as is possible, that it is accurate and up to date. Personal information should be checked at regular intervals, to make sure that it is still accurate and up to date. If the information is found to be inaccurate, steps must be taken to put it right. Individuals who input or update information must also make sure that it is adequate, relevant, clear and professionally worded.

7.2. ‘Data subjects’ have a right to access personal information held about them and have errors corrected. More information about a ‘data subject’s’ rights can be found in Section 9 of this policy.

8. Retention and Disposal of Information

8.1 Telford & Wrekin Council holds a large amount of personal information. The GDPR requires that we do not keep personal information for any longer than is necessary. Personal information should be checked at regular intervals and deleted or destroyed securely when it is no longer needed, provided there is no legal or other reason for holding it.

8.2 The Corporate Information Retention Schedule must be checked before records are disposed of, to make sure that the prescribed retention period for that type of record is complied with. Alternatively advice should be sought from Information Governance.

9. Individuals Rights

9.1. Individuals have a number of rights under GDPR. These include:

- **The right to be informed** – See section 4 - Collecting Personal Information
- **The right to access** – A person can ask for a copy of personal information held about them (this is known as a Subject Access request - SAR);
- **The right to rectification** – Personal data can be rectified if it is inaccurate or incomplete
- **The right to erasure** – Person can ask for the deletion or removal of personal data where there is no reason for its continued processing
- **The right to restrict processing** – Person has the right to block or suppress processing of their personal data
- **The right of data portability** – Allows a person to obtain and reuse their personal data for their own purposes
- **The right to object** – A person can object to an organisation processing their personal data for direct marketing, on the basis of legitimate interests or for scientific/historical reseach and statistics
- **Rights related to automated decision making/profiling** – A person can ask for human intervention in an automated process

9.2 If any Council service receives such a request on any of the above matters they should seek advice from the Information Governance Team.

9.3 The Council has one calendar month in which to respond to a SAR, provided the applicant has put their request in writing by completing a subject access request form and suitable proof of identification has been supplied. An extension of a further 1-2 months will be applied where a request is deemed complex The Information Governance Team co-ordinates the processing of all SAR requests. ***See Appendix 2*** for a copy of the SAR form.

10. Reporting Security Incidents

10.1 Telford & Wrekin Council has a responsibility to monitor all incidents that occur within the organisation that may breach the security and/or the confidentiality of its information. All incidents need to be identified, reported, investigated and monitored. It is only by adopting this approach that the Council can learn from its mistakes and prevent losses recurring.

10.2 Specific procedures have been developed for the reporting of all information security incidents. It is designed to make sure that all relevant information is communicated correctly so that timely corrective action can be taken. The documents below need to be read, understood and followed:

- Information Security Breach Procedure – under 'I' on intranet
- Data Breach Investigation – under 'D' on intranet

10.3 All employees (permanent, temporary and contractors) must be aware of the procedures and obligations in place for reporting the different types of incidents which may have an impact on the security of the Council's information.