Council Name: Sandhurst Town Council
Council Address: Council Offices, Memorial Park, Yorktown Road, Sandhurst, Berks GU47 9BJ
Email Address: stc@sandhurst.gov.uk
Telephone numbers: 01252 879060

DATA PROTECTION POLICY

1. Introduction

The General Data Protection Regulations (GDPR) and the Data Protection Act 2018 (DPA 2018) amend and update the existing framework of rights and duties which safeguard personal data. Personal data is information about a living individual (a data subject) who can be identified from such data, and should be broadly interpreted, as it encompasses not only names and addresses, but can include photographs, email addresses, and digital data such as IP addresses and cookie identifiers. This legal framework balances the legitimate needs of organisations to collect and use personal data for business and other purposes, against the right of individuals to respect for the privacy of their personal data.

Sandhurst Town Council is committed to protecting the privacy of individuals and handles all personal data in a manner that complies with the GDPR and the DPA 2018. The Council has established the following policy to support this commitment. It is the personal responsibility of all employees, Members, contractors, agents and anyone else processing information on behalf of the Town Council to comply with this policy. This policy continues to apply to employees and individuals even after their relationship with the Council ends.

Any deliberate breach of this policy could amount to a criminal offence under one or more pieces of legislation. All incidents will be investigated and action may be taken by the Council's formal disciplinary procedure. A serious breach of this policy could be regarded as gross misconduct and may lead to dismissal and/or criminal action being taken.

2. Data Protection Principles (Article 5)

The GDPR are underpinned by a set of seven common-sense Principles, which must be adhered to whenever personal data is processed. Processing includes obtaining, recording, using, holding, disclosing and deleting personal data.

- Processing must be lawful, fair and transparent.
- The purposes for which data is processed must be specific, explicit and legitimate.
- Data which is processed must be limited to what is adequate and relevant. If depersonalised information is sufficient, personal data must not be collected.
- Data which is processed must be accurate and kept up to date.
- Data must be retained no longer than is necessary.
- Data must be kept securely and protected against unauthorized access, theft or loss.
- The Data Controller must be responsible for and able to demonstrate their compliance with these Principles, (accountability).

3. Lawful basis for processing (Article 6(1))

When Sandhurst Town Council processes personal data, it must have a lawful basis for doing so. Processing is only lawful if at least one of the conditions below is met.

- Consent – which must be a freely given, specific, informed and unambiguous indication of the data subject's wishes, and signified by a statement or a clear affirmative action.
- Contract – with the data subject. Examples might be data processed for a contractual obligation such as hall hire, cemetery records, or allotment rentals.
- Legal obligation – of the Data Controller. An example might be disclosing salary details of employees to HMRC. It also covers dealing with complaints, planning matters and FoI enquiries.
- Vital interests – of the data subject or someone else. An example might be providing information about elderly residents to local emergency services in a civil emergency such as a fire or flood.
- Public Interest – processing carried out for the performance of a task in the public interest, which includes the exercise of a function conferred on a person by an enactment or rule of law, and an activity that supports or promotes democratic engagement – an example is canvassing on behalf of elected members.

Because in most cases the lawful basis for processing is 'informed consent', the data subject (the person who the information is about) must be told, unless this is obvious to them, which organisation(s) they are giving their information to; what their information will be used for; who it may be shared with, how it will be safeguarded, and how long it will be held, as well as anything else that might be relevant e.g. the consequences of that use. A formal notice, known as a Privacy Notice, can be used to provide this information.

If the personal data is collected for one purpose, it must not subsequently 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 at the time the information is collected what other purposes their information may be used for.

4. Special Categories of Personal Data (Article 9)

The old Data Protection Act 1998 identified 'sensitive' personal data, which required higher levels of protection and consent. The GDPR has revised and broadened this definition,and reclassified the data as 'Special Categories of Personal Data'. Sandhurst Town Council will process the Special Categories of Personal Data in compliance with the provisions of the GDPR.

Special Categories of Personal Data are defined as: Racial or ethnic origins; Political opinions; Religious or philosophical beliefs; Trade-Union membership; Genetic or biometric data; Health data; and Sexual orientation or sex life.

Criminal data, which was previously included as sensitive data, is not included in the GDPR. This is because the DPA 2018 and other legislation such as the Regulation of Investigatory Powers Act (RIPA) cover criminal data. Only organisations with specific authority under Article 6 can process criminal data.

Special Categories of Data can only be processed if one of the following conditions are met:

- The data subject has given explicit consent,
- The data subject has made the data public,
- The data is held for certain employment reasons,
- The data is used to protect vital interests,
- For a foundation or association with a specific aim (like a trade-union or a religious group for example),
- For proportionate public interest reasons
- For various health reasons,
- Or for historic archiving purposes.

Examples for Town councils might include employment records, equalities surveys, or people's political opinions collected during electoral canvassing, when such data compilation is permitted, with safeguards.

5. Access to and use of personal data

Access to and use of personal data held by the Council is only permitted by employees, Members, contractors and agents and anyone else processing information on behalf of the Town Council for the purpose of carrying out their official duties. Processing for any other purpose is prohibited.

Deliberate unauthorised access to, copying, disclosure, destruction or alteration of or interference with any computer equipment or data is strictly forbidden and may constitute an offence under S148 of DPA 2018, and/or a disciplinary offence.

It is an offence under Section 170(1) of the DPA 2018 for any person to knowingly or recklessly obtain, procure or disclose personal data without the permission of the Data Controller (Sandhurst Town Council) subject to certain exceptions. It is also an offence for someone to sell or offer to sell personal data which has been obtained in contravention of S170(1).

It is an offence under S173 of DPA 2018 to alter, deface, erase, block or conceal personal data from the data subject to prevent disclosure.

The Information Commissioner (the Regulator for Data Protection) has a range of powers to regulate and enforce lawful processing of personal data. These include access to records held by Sandhurst Town Council if required.

6. Disclosing personal data

Personal data must not be disclosed to anyone internally or externally unless the person disclosing the information is fully satisfied that the enquirer or recipient is authorized in all respects and is legally entitled to the information.

If personal data is disclosed to another organization or person outside of the Town Council, the disclosing person must identify their lawful basis for the disclosure and record their decision. This should include a description of the information disclosed; the name of the person and organization to which the information was disclosed; the date; the reason for the disclosure; the lawful basis.

In response to any lawful request, only the minimum amount of personal information should be disclosed. The person disclosing the information should ensure that the information is adequate for the purpose of the disclosure, relevant and not excessive.

7. Accuracy and relevance

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

Data subjects have a right to access personal data held about them and have inaccuracies corrected. More information about a data subject's rights can be found in Section 9 below.

8. Retention and disposal of personal data

Personal data should be held only for as long as it is required for the purpose for which it was collected. To facilitate this Sandhurst Town Council holds a Record Retention Schedule/Record Management Policy which provides guidance on prescribed retention periods for the personal data and other information which it holds. Personal data must be deleted or destroyed in a secure fashion.

Sandhurst Town Council also holds a Record of Processing Activities which sets out the categories of personal data it processes, and the individuals or organisations with which this data is shared.

9. Individual Rights

Under GDPR individuals have a number of rights which allow them to ensure that their data is being processed lawfully. These rights are:

- Right to transparency – Privacy Notices and other information about how personal data is processed.
- Right of access - subject access requests.
- Right to rectification – correction of inaccurate data.
- Right to erasure – the ‘right to be forgotten’.
- Right to object to processing – in cases of direct marketing
- Automated decisions and profiling
- Right of data portability

Subject access requests (an individual’s request for their own personal data), can be made in writing or verbally, provided the applicant has provided suitable identification. Third parties can also make requests on behalf of others, a process which requires additional checks to ensure lawful access. In most

cases there is no fee for a request.

Requests made via Members must be passed to the Executive Officer to progress as soon as possible. Town Council has one calendar month in which to respond to a Subject Access request If the Town Council holds a considerable amount of personal data on this individual the timescale can be extended by up to a further two calendar months, but in such cases the individual must be kept informed, and the Town Council must still process the request as quickly as possible.

In response to a subject access request the Town Council must provide copies of the data, information on the source of the data (unless this is obvious from the context), information on how it is processed and for what purposes, and information on the retention period. Information should be provided electronically where possible, and appropriate checks must be carried out to ensure that the correct email address is used when supplying personal data.

10. Data breaches and data security

Security of personal data is paramount. Sandhurst Town Council has a legal obligation to monitor all incidents that occur within the organization which may breach the security and/or confidentiality of the information it holds. All incidents must be identified, reported, investigated and monitored. Serious breaches of personal data security must be reported to the Information Commissioner.

Sandhurst Town Council will use secure systems at all times to ensure the security of personal data and confidential information. This includes security of electronic and paper records, the secure use of IT systems, and the security of records in transit.

11. Registration

Town Councils are required to register with the Information Commissioner to process personal data. Sandhurst Town Council is registered to process personal data.