Chippenham Town Council

Improving the quality of town life

Data Protection Policy

Chippenham Town Council

Approved and adopted by:
Strategy and Resources Committee

Date policy was adopted: 13.06.18

Review date: 13.06.21

Updates

Amendments which do not require a policy review

Date:

Detail:

Contents

1 Change Control

This Policy was created in	May 2018
Council Staff were consulted on this document and it was accepted on	
It was ratified by the Council on	
Renewal data	April 2019
This version is	Version 1.0
It replaces	No previous version
It is necessary to comply with	Data Protection Act 1998 General Data Protection Regulation 2016

2 Definitions

Data Protection Act 1998 ("DPA")	The law on data protection in the UK
General Data Protection Regulation ("GDPR")	A new law on data protection that comes into force on 25 May 2018 throughout Europe
Data Controller	A person or organisation that handles and processes personal data and determines the way such data should be processed
Personal Data	Any information from which a living individual can be identified
Sensitive Personal Data	Any Personal Data which includes further information as defined in the DPA. Further information includes (i) racial or ethnic origin; (ii) political opinions; (iii) religious beliefs; (iv) membership of a trade union; (v) physical or mental health or condition; (vi) sexual life or preferences; (vii) information about any criminal offence or court proceedings related to a criminal offence
Information Commissioner's Office ("ICO")	The statutory regulator of the DPA and the GDPR
Privacy Notice	A description of Personal Data held by the Council, along with details of purpose, retention and other information about how the Council will handle the Personal Data
Data Subject	As defined in the DPA and the GDPR. The Data Subject is the person who the Personal Data is about, or who is identified by the Personal Data

3 Mission Statement

Chippenham Town Council ("the Council") is a town council representing the local community, delivering services to meet local needs and improving the quality of town life for all.

In order to make this happen, the Council collects and uses Personal Data about residents, staff, volunteers, councillors and other individuals who all play their part in being part of the community. This information is gathered in order to enable the Council to provide a rich and broad service. In addition, there may be a legal requirement to use information for the purpose of sharing it with other organisations. In some cases, the Council must collect information to ensure that it complies with statutory obligations.

The Council holds large amounts of personal and sensitive data. It is responsible for safeguarding the data it holds and is legally bound under the GDPR to ensure the security and confidentiality of personal information processed. These responsibilities extend to other organisations working on behalf of the Council.

3.1 Purpose

This Policy is intended to ensure that Personal Data is dealt with correctly and securely and in accordance with the DPA, GDPR and other related legislation. It will apply to information regardless of how it is collected, used, recorded, stored and destroyed or deleted, and irrespective of whether it is held in paper files or electronically.

Everyone involved with the collection, processing and disclosure of Personal Data will be aware of their duties and responsibilities by adhering to these guidelines.

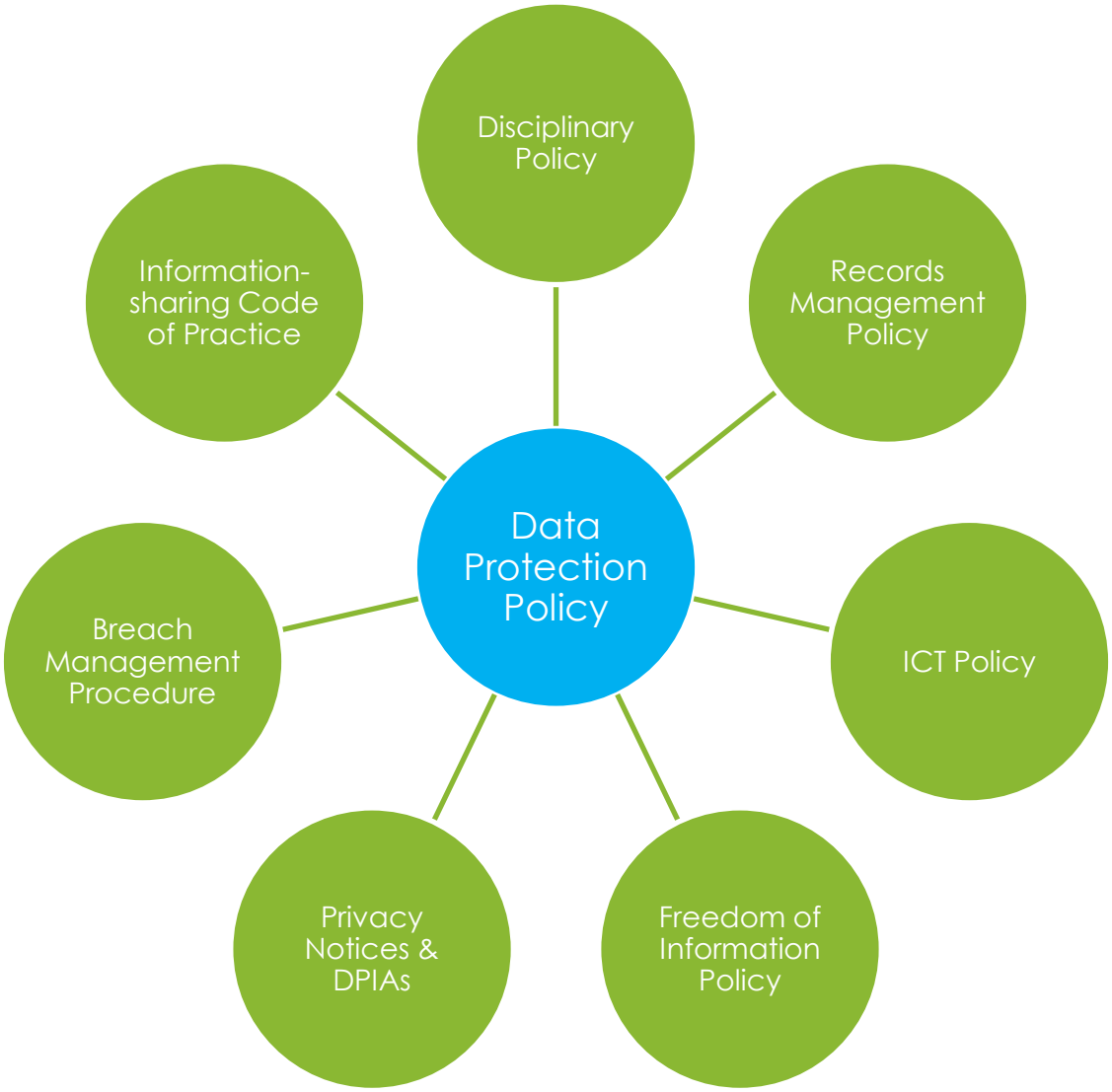
This Policy is central to the Council's suite of policies designed to ensure that the Council is compliant with the DPA and GDPR in all aspects of its work where Personal Data is handled.

The spidergram in the next section shows how this Policy interacts with those other policies.

Staff and councillors are expected to adhere to the principles and spirit of this Policy to protect Personal Data belonging to our residents, friends of the Council and members of staff. Anyone found to have breached this Policy may find that the Council will invoke the Disciplinary Procedure.

This Policy has been approved by the elected members of the Council, and is evidence of the commitment the Council makes to safeguarding Personal Data.

4 Spidergram of Policies



5 Data Protection Principles

The GDPR establishes enforceable principles that must be adhered to at all times:

1. Personal Data must be lawfully and fairly processed, in a transparent manner
2. Personal Data shall be obtained only for specified and explicit purposes
3. Personal Data shall be adequate, relevant and not excessive
4. Personal Data shall be accurate and kept up to date
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes
6. Personal data shall be kept secure and protected by appropriate technical and organisational measures
7. A data controller must be able to demonstrate compliance with these principles

The Council is committed to maintaining the above principles at all times. Therefore the Council will:

- Inform individuals why Personal Data is being collected and when
- Inform individuals when their information is shared and why and with whom
- Check the quality and the accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with individuals' rights
- Ensure our staff and councillors are aware of and understand our policies and procedures

6 Fair & Lawful Processing

The Council needs to collect and handle Personal Data for a number of reasons.

Residents and customers

- name, address, contact details
- Purchasing history where events are booked at the Neeld Hall and Chippenham Museum or at the information centre
- Planning information where an application has been made
- Photographs at events for encouraging community participation and promotional purposes
- CCTV used in the town centre

Staff

Data is held about staff. This includes:

- name, address, phone number, next of kin, emergency contact details
- car insurance details, car registration number
- bank details, earnings from other sources or previous employer, pensions data
- DBS number and date authorised (including spent and unspent convictions)
- medical details, including records of sickness absence and maternity/paternity
- work history, educational history, references
- ethnicity, sexuality, personal living arrangements
- criminal offences/cautions relating to themselves and their partners
- nationality, right to work, and forms of ID (passports, driving licence, birth certificates)
- Performance data, disciplinary records
- Photograph

This data is held to enable the Council to comply with its legal obligations and to ensure safeguarding requirements are met.

Elected members

- name, address, phone number, email address,
- car insurance details

- bank details, earnings from other sources or previous employer
- medical details (for those aged over 80 for insurance purposes)
- any interests or information they have declared in their Declaration of Interests
- political views and membership details
- Photographs

Volunteers

- name, address, phone number, next of kin, emergency contact details
- DBS number and date authorised (including spent and unspent convictions)
- work history, educational history, references
- Photograph

Visitors and others

From time to time, there will be visitors to the Council. They will be asked to provide their names and contact details.

Contractors' details will also be stored. This includes their name, the organisation they work for, and contact details. In some cases, we will retain their insurance documentation.

Other visitors will be required to sign in, thus providing their name and organisation details.

Information regarding community groups may consist of Personal Data where these are provided as part of the Council's relationship with the community group.

Information consisting of Personal Data may also be shared with law enforcement agencies, such as the Police, from time to time in order to assist them with the prevention and detection of crime.

If the Council collect data for any other purposes, or from any other person, the Council will ensure that the purpose of the processing of that data is clear and where necessary, consent is obtained in advance.

Data security

Regardless of the purpose, Personal Data will always be held securely. If in paper format, Personal Data will always be held in secure rooms with access only to authorised individuals. If in electronic format, Personal Data will be stored on password-protected computers belonging to the Council.

7 Accuracy of Personal Data

Under data protection law, the Council is required to ensure that Personal Data is kept accurate and up-to-date. To comply with the applicable law, the Council will:

- Take reasonable steps to ensure the accuracy of any Personal Data that is obtained;
- Ensure that the source of any Personal Data is clear;
- Carefully consider any challenges to the accuracy of Personal Data; and
- Consider where necessary if Personal Data needs to be updated or rectified

If a Data Subject informs the Council of a change of circumstances, or notifies the Council of an error, inaccuracy or defect in the Personal Data held, the Council will update both paper and electronic records as soon as practicable. This will normally be done within one month.

Where a Data Subject challenges the accuracy of the data, the Council will immediately mark the record as potentially inaccurate. In the case of any dispute, the Council will try to resolve the issue informally but if this is not successful, disputes will be referred to the Chief Executive for a decision.

8 Retention of Records

This section sets out a brief framework for management decisions on whether a particular document (or set of documents) will either be:

- Retained – and if so in what format and for what period
- Disposed of – and if so by when and by what method

More information about how we retain records including the retention periods is available by viewing our Records Management Policy.

Residents' records

Residents' records will be collected for a number of reasons. DPIAs will always document the purpose for the processing of these records. The periods of retention are contained within the Records Management Policy. Staff will always consult that Policy when deciding how long to retain this information. This will depend on the purpose of the information collected.

Staff records

These will be retained through the employment of the employee, and for 6 years following the termination of employment.

All other Personal Data falling outside of these periods will be securely destroyed.

All records that are to be retained will be retained securely in a secure cupboard with limited access and only to key authorised individuals. The Head of Finance and Administration will determine the basis for individuals to have access to this information.

Destruction of records

Where paper records are identified as needing to be destroyed, these will be shredded securely by the relevant provider procured by the Council. Currently destruction of records takes place onsite using shredders.

9 Data Subject Rights

9.1 General principles

The Council is open and transparent about the data that it processes. A number of rights are available to individuals, as set out below.

Requestors are encouraged to use the form at Annex 1 to make their request. Any requests for CCTV footage should be completed using the form contained within the CCTV Code of Practice.

Parental rights

Children under the age of 16 are deemed not to have the mental capability to understand what an SAR is to be able to make a request themselves, by virtue of their age. However, they are still entitled to make requests regarding their data.

Normally those with parental responsibility for a child will be the only individuals able to make a DSR to the Council for that child's information. They will be deemed to be acting in the child's best interests unless the Council has grounds to believe otherwise. The Council is obliged to disclose this information on request to that person.

However, if the Council believes that a person with parental responsibility is making a DSR not in the child's best interests, but for some other purpose, it will decline to provide any information to that person. In these cases, the Council will confirm the same to the requestor. This may be particularly relevant where those with parental responsibility are in legal proceedings against each other, for example, divorce.

Appeal

The Council provides requestors with a right of appeal should they be dissatisfied with the way their DSAR has been handled. Requestors should lodge their appeal with the Chief Executive within 5 working days of any documentation being received (if that is the nature of their complaint), or within 10 Council days of the expiry of a deadline to provide information.

9.2 The right to be informed

An individual has the right to be informed about the use and collection of their personal data. We provide this information through a series of Privacy Notices, which are on our website. You can view these by visiting www.chippenham.gov.uk and following the links to our Privacy Notices and data protection pages.

9.3 Subject Access Requests (SARs)

A Subject Access Request is the right of any individual to access information held about them by the Council.

SAR regime

An SAR can be made by a person by writing to the Corporate Support Manager at the Council. The Council is entitled to see appropriate proof of ID to satisfy itself of the identity of the person making the request.

Once the Council is satisfied with identity of the requestor, the Council must provide the information within 30 days of receiving the proof of ID.

Note that if disclosure of any records is likely to infringe the following, then the Council is not obliged to disclose:

- Information that would cause serious harm to the physical or mental health of any person
- Information contained in adoption or parental order records

Disclosure of records

The Council will contact the requestor once the information is ready for disclosure. The Council requires that given the sensitivity of the documentation generally, the requestor will be asked to collect the information from the Council. Only if the requestor declines and can confirm in writing that he/she is content for the Council to post the information by "signed for" first class delivery by Royal Mail, then the Council will despatch the information by post. Information to be sent abroad will be sent by standard air mail.

Requestors may wish to have the information sent to them by a postal method even more secure than the route outlined above. If so, requestors should state this clearly on their request. Requestors will need to pay for this if there is an increase in the cost compared to the routes outlined above.

Redaction

Sometimes it will not be possible to disclose Personal Data under an SAR without breaching the Personal Data of a third party. This might be another resident for example. In such cases, where possible, the Council will redact the Personal Data of the third party from any documents to be disclosed. However, often, by redacting third party Personal Data the document is left looking nonsensical and cannot reasonably be disclosed. On these occasions, the document will not be disclosed at all to the requestor.

Exemptions

There are a number of exemptions from disclosing Personal Data under an SAR:

1. The information consists of confidential references
2. The information consists of publicly available information
3. The information if disclosed would prejudice the prevention or detection of crime, the capture or prosecution of offenders or the assessment or collection of tax or any duty
4. The information consists of management information, including management forecasting or management planning
5. The information consists of negotiations with the requestor and disclosure would be likely to prejudice those negotiations

6. The information consists of regulatory activity
7. The information consists of legally privileged information
8. The information consists of information that is requested in connection with actual or potential legal proceedings
9. The information consists of social work records and disclosure would be likely to prejudice that work

Any complaint about an SAR should be directed to the Chief Executive within 14 days of the date that the information was sent, or in the case of a complaint about a delay in sending the information, within 14 days of the intended date that the information was due to be sent.

9.4 Right to rectification and restriction of processing

Individuals have the right to have inaccurate data corrected, or to have incomplete data completed.

When we receive a request, we will consider it carefully. The more important it is that the data is accurate or complete, the more detailed our consideration will be.

We will aim to provide a response within one month. On occasions, we may require a further two months to respond. We will keep the requestor informed if this is the case.

Data that is inaccurate means that it is incorrect or misleading as to any matter of fact. This doesn't apply to opinions that are provided as these are subjective.

At the point that we receive a request to rectify data, we will halt the processing of that data until such point as a decision is made and the data – where inaccurate or incomplete – is rectified. An individual can also make a request that we restrict processing of their data even where there is no request to rectify.

There are some exemptions to rectifying data or restricting processing of data, and as such it is not an absolute right.

If a request is manifestly unreasonable to comply with, we will explain our justification and either take no further action, or ask the requestor to pay a fee to cover the administrative costs of the rectification.

9.5 Right to be forgotten

Under the GDPR, individuals have the right to request the Council to delete Personal Data where there is no compelling reason for them to retain it:

- Where the Personal Data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (i.e. otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.

- The personal data is processed in relation to the offer of information society services to a child.

An individual may make a request by writing to the Corporate Support Manager if they wish to request the Council delete or remove any Personal Data. The Council will consider such a request and within 20 Council days will either confirm the deletion or removal of all Personal Data (other than retaining a record of the request itself) or will inform the individual that the Personal Data will not be deleted, because it is required for one of the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- for public health purposes in the public interest;
- archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- the exercise or defence of legal claims.

We may also refuse a request where it is manifestly unreasonable, or where it is repetitive, and in these circumstances we may request a fee to cover our administrative costs.

9.6 Right to object to processing

Individuals have a right to object to processing of data where it is done for direct marketing purposes, where the processing is a task carried out in the public interest, or where there is a legitimate interest.

The Council will normally respond within one month of receiving such a request.

There are some exceptions to this right, and we will inform requestors if we decline their request providing reasons.

10 Information Security

The Council will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, Personal Data.

The Council will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal Data will only be transferred to a data processor if it agrees to comply with those procedures and policies, or if it puts in place adequate measures himself.

The Council will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

Confidentiality means that only people who are authorised to use the data can access it.

Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.

Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal Data is therefore stored on the Council's central computer system instead of individual PCs.

Security procedures include:

- Entry controls. Any stranger seen in entry-controlled areas should be reported.
- Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
- Methods of disposal. Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required. Electronic data is wiped.
- Equipment. Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

11 Training & Development

The Council is committed to ensuring the staff adopt the highest standards in relation to the processing and handling of Personal Data.

All existing staff will be trained within 6 months of the dissemination of this Policy.

New staff (and councillors) will be trained as part of their induction within 3 months of their joining the Council and being able to access Personal Data.

Staff will be re-trained according to their needs against the tide of new guidance and legislation. It is anticipated that this will usually be annually.

No member of staff will have access to any Personal Data unless they have read this Policy first.

12 Further Information

Any person reading this Policy requiring further information or assistance is invited to contact the Council's Data Protection Officer at dpo@chippenham.gov.uk.

Where any person has a complaint about the way the Council has handled their Personal Data or that of their child's, they may address their concern in writing to the Chief Executive.

For further information about the DPA, GDPR and its application, the Information Commissioner's Office has a wealth of information on its website – www.ico.org.uk

Annex 1 – DSR template

Proof of authority

If you are asking for information about someone else you must provide us with written evidence that you have the authority to act for that person. It can include proof of guardianship and power of attorney.

Proof of identity

Evidence of your identity and address must be provided by sending us originals or certified copies of at least two official documents. This must also be provided for the person about whom information is required and the person making the request if they are different.

- Proof of identity – birth certificate, current driving licence or passport identification page
- Proof of address – current driving licence, utility bill, bank or credit card statement (less than three months old)

What is acceptable

The Council accept copies of original documents however, the Council reserve the right to request to see the physical original documentation in some cases. All original documents will be returned.

The personal information you provide on this form will only be used by the Council for the purpose of locating any information that you are requesting access to. By submitting this application form you are consenting to the Council using information provided for this purpose. After completion the information will be retained for a period of two years.

Data Subject Request (DSR) Form

Your details ("the Requestor")

Full name:
Previous name (if applicable):
Date of birth (DD/MM/YYYY):
Present address:

Email:

Telephone number:

Details of the person on whom information is being requested (the "data subject"), <u>if different to above</u>:

Full name:
Previous name (if applicable):
Date of birth (DD/MM/YYYY):
Present address:

Email:

Telephone number:

Please tick which request you would like to make:

□ Subject Access Request

□ Right to rectification and restriction of processing

□ Right to be forgotten

□ Right to object to processing

Please give us a brief description of your request and reasons for it

For SARs: **Details required** *It will help speed up the process if you tell us the period for which it is required. Please also try to name the service of the council that you think might hold the information.* **Period of time to be searched** **Dates (DD/MM/YY to DD/MM/YY):** **List different addresses used during this period**
If you do not wish to collect the resulting paperwork from the Council, please indicate the method of transmission: *(Please note you will be asked for an additional payment to cover any increase in postage costs)*
Any further information you believe is relevant?