WENDOVER PARISH COUNCIL
The Clock Tower, High Street, Wendover,
Aylesbury, Buckinghamshire HP22 6DU
Tel: 01296 623056 Email: clerk@wendover-pc.gov.uk

Data Protection Policy

Wendover Parish Council (the Council) processes personal data about our employees, clients, customers and other individuals for a variety of business purposes and in the exercise of official authority. This might include names, addresses, telephone numbers etc.

This policy sets out how the Council seeks to protect personal data and ensure that staff and council members understand the rules governing their use of personal data to which they have access in the course of their work.

This policy is underpinned by the Data Protection Act 2018 and the retained EU General Data Protection Regulations (GDPR) and is informed by guidance from the Information Commissioner's Office (ICO).

This policy contains:

- the data protection principles with which the Council must comply;
- what is meant by personal information (or data) and sensitive personal information (or data);
- how we gather, use and (ultimately) delete personal information and sensitive personal information in accordance with the data protection principles;
- where more detailed privacy information can be found, e.g. about the personal information we gather and use about you, how it is used, stored and transferred, for what purposes, the steps taken to keep that information secure and for how long it is kept;
- your rights and obligations in relation to data protection;
- the consequences of failure to comply with this policy.

The appendices contain:

- The privacy notices (for the general public and the staff/Councillors)
- The details of the data we collect, store and process and the legal basis for that

Policy Statement

- Wendover Parish Council in the course of its work will collect, process and store personal data. The Council takes this seriously and is committed to meeting its obligations under the Data Protection Act 2018 and the retained EU General Data Protection Regulations (GDPR)
- Wendover Parish Council will seek to follow best practice for data protection as set out in guidance to the sector and from the Information Commissioners Office.

Other linked policies:
Information Security Policy

WENDOVER PARISH COUNCIL
The Clock Tower, High Street, Wendover,
Aylesbury, Buckinghamshire HP22 6DU
Tel: 01296 623056 Email: clerk@wendover-pc.gov.uk

Implementation of the policy

1 Introduction

1.1 The Council obtains, keeps and uses personal information (also referred to as data) about, for example, job applicants, Councillor contact details, allotment tenants and sets out privacy notices that set out how this data is used and the data table sets out in detail the data we store and process and our legal basis for doing so.

1.2 This policy sets out how the Council complies with its data protection obligations and seeks to protect personal information. Its purpose is also to ensure that staff understand and comply with the rules governing the collection, use and deletion of personal information to which they may have access in the course of their work.

1.3 The Council is committed to complying with its data protection obligations, and to being concise, clear and transparent about how it obtains and uses personal information relating to its workforce, and how (and when) it deletes that information once it is no longer required.

1.4 The Council will nominate a data protection lead who will be the Clerk unless otherwise specified. The data protection lead is responsible for informing and advising the Council and its staff on its data protection obligations, and for monitoring compliance with those obligations and with the Council's policies. If you have any questions or comments about the content of this policy or if you need further information, you should contact the data protection lead at the Clock Tower.

2 Scope

2.1 This policy applies to any personal information that the Council collects, processes and stores as set out in the appendices

2.2 Staff should also refer to the Council's Information Security Policy.

2.3 The Council will review and update this policy in accordance with its data protection obligations. It does not form part of any employee's contract of employment and the Council may amend, update or supplement it from time to time. The Clerk will circulate any new or modified policy to staff when it is adopted.

3 Definitions

criminal records information	means personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures;
data breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information;
data subject	means the individual to whom the personal information relates;
personal information	(sometimes known as personal data) means information relating to an individual who can be identified (directly or indirectly) from that information;
processing information	means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with it;
pseudonymised	means the process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable individual;
sensitive personal information	(sometimes known as 'special categories of personal data' or 'sensitive personal data') means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics

	information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

4 Data protection principles

4.1 The Council will comply with the following data protection principles when processing personal information:

4.1.1 we will process personal information lawfully, fairly and in a transparent manner;

4.1.2 we will collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;

4.1.3 we will only process the personal information that is adequate, relevant and necessary for the relevant purposes;

4.1.4 we will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information are deleted or corrected without delay;

4.1.5 we will keep personal information in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the information is processed; and

4.1.6 we will take appropriate technical and organisational measures to ensure that personal information are kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

5 Basis for processing personal information

5.1 In relation to any processing activity the Council will, before the processing starts for the first time, and then regularly while it continues.

5.1.1 review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing, i.e.:

(a) that the data subject has consented to the processing;

(b) that the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) that the processing is necessary for compliance with a legal obligation to which the Council is subject;

(d) that the processing is necessary for the protection of the vital interests of the data subject or another natural person;

(e) that the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority;

(f) that the processing is necessary for the purposes of legitimate interests of the Council or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject—see clause 5.2 below.

5.1.2 except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose);

5.1.3 document its decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;

5.1.4 include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s);

5.1.5 where sensitive personal information is processed, also identify a lawful special condition for processing that information (see paragraph 6.2.2 below), and document it; and

5.1.6 where criminal offence information is processed, also identify a lawful condition for processing that information, and document it.

5.2 When determining whether the Council's legitimate interests are the most appropriate basis for lawful processing, it will:

5.2.1 conduct a legitimate interest assessment (LIA) and keep a record of it, to ensure that we can justify our decision;

5.2.2 if the LIA identifies a significant privacy impact, consider whether it also needs to conduct a data protection impact assessment (DPIA);

5.2.3 keep the LIA under review, and repeat it if circumstances change; and

5.2.4 include information about its legitimate interests in the relevant privacy notice(s).

6 Sensitive personal information

6.1 Sensitive personal information is sometimes referred to as 'special categories of personal data' or 'sensitive personal data'.

6.2 The Council may from time to time need to process sensitive personal information. It will only process sensitive personal information if:

6.2.1 It has a lawful basis for doing so as set out in paragraph 5.1.1 above, e.g. it is necessary for the performance of the employment contract, to comply with the Council's legal obligations or for the purposes of the Council's legitimate interests; and

6.2.2 one of the special conditions for processing sensitive personal information applies, e.g.:

(a) the data subject has given has given explicit consent;

(b) the processing is necessary for the purposes of exercising the employment law rights or obligations of the Council or the data subject;

(c) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;

(d) processing relates to personal data which are manifestly made public by the data subject;

(e) the processing is necessary for the establishment, exercise or defence of legal claims; or

(f) the processing is necessary for reasons of substantial public interest.

6.3 Before processing any sensitive personal information, staff must notify the Clerk of the proposed processing, in order that the Clerk may assess whether the processing complies with the criteria noted above. If the Clerk is in any doubt they must seek appropriate advice.

6.4 Sensitive personal information will not be processed until:

6.4.1 the assessment referred to in paragraph 6.3 has taken place; and

6.4.2 the individual has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

6.5 The Council's data protection privacy notices sets out the types of sensitive personal information that the Council processes, what it is used for and the lawful basis for the processing.

7 Data protection impact assessments (DPIAs)

7.1 Where processing is likely to result in a high risk to an individual's data protection rights (e.g. where the Council is planning to use a new form of technology), it will, before commencing the processing, carry out a DPIA to assess:

7.1.1 whether the processing is necessary and proportionate in relation to its purpose;

7.1.2 the risks to individuals; and

7.1.3 what measures can be put in place to address those risks and protect personal information.

7.2 Before any new form of technology is introduced, the manager responsible should therefore contact the Clerk in order that a DPIA can be carried out.

7.3 During the course of any DPIA, the employer will seek the advice of the Clerk and the views of a representative group of employees and any other relevant stakeholders.

7.4 A checklist for whether to employ a DPIA is included in Appendix C

8 Documentation and records

8.1 The Council will keep written records of processing activities which are high risk, i.e. which may result in a risk to individuals' rights and freedoms or involve sensitive personal information or criminal records information, including:

8.1.1 the name and details of the employer's organisation (and where applicable, of other controllers, the employer's representative and DPO);

8.1.2 the purposes of the processing;

8.1.3 a description of the categories of individuals and categories of personal data;

8.1.4 categories of recipients of personal data;

8.1.5 where possible, retention schedules; and

8.1.6 where possible, a description of technical and organisational security measures.

8.2 As part of its record of processing activities the Council will document, or link to documentation, on:

8.2.1 information required for privacy notices;

8.2.2 records of consent;

8.2.3 controller-processor contracts;

8.2.4 the location of personal information;

8.2.5 DPIAs; and

8.2.6 records of data breaches.

8.3 If the Council processes sensitive personal information or criminal records information, it will keep written records of:

8.3.1 the relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose;

8.3.2 the lawful basis for its processing; and

8.3.3 whether the Council retains and erases the personal information in accordance with its policy document and, if not, the reasons for not following its policy.

8.4 The Council will conduct regular reviews of the personal information it processes and update its documentation accordingly. This may include:

8.4.1 carrying out information audits to find out what personal information the Council holds;

8.4.2 distributing questionnaires and talking to staff across the Council to get a more complete picture of our processing activities; and

8.4.3 reviewing its policies, procedures, contracts and agreements to address areas such as retention, security and data sharing.

9 Privacy notice

9.1 The Council will issue privacy notices from time to time, informing you about the personal information that it collects and holds relating to you, how you can expect your personal information to be used and for what purposes.

9.2 The Council will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

WENDOVER PARISH COUNCIL
The Clock Tower, High Street, Wendover,
Aylesbury, Buckinghamshire HP22 6DU
Tel: 01296 623056 Email: clerk@wendover-pc.gov.uk

10 Individual rights

10.1 Data Subjects have the following rights in relation to your personal information:

10.1.1 to be informed about how, why and on what basis that information is processed—see the Council's data protection privacy notice;

10.1.2 to obtain confirmation that your information is being processed and to obtain access to it and certain other information, by making a subject access request—see the Council's subject access request policy;

10.1.3 to have data corrected if it is inaccurate or incomplete;

10.1.4 to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as 'the right to be forgotten');

10.1.5 to restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased), or where the employer no longer needs the personal information but you require the data to establish, exercise or defend a legal claim; and

10.1.6 to restrict the processing of personal information temporarily where you do not think it is accurate (and the employer is verifying whether it is accurate), or where you have objected to the processing (and the employer is considering whether the organisation's legitimate grounds override your interests).

10.2 If you wish to exercise any of the rights in paragraphs 10.1.3 to 10.1.6, please contact the Clerk.

11 Individual obligations

11.1 Individuals are responsible for helping the Council keep their personal information up to date. You should let the Clerk know if the information you have provided to the Council changes, for example if you move house or change details of the bank or building society account to which you are paid.

11.2 You may have access to the personal information of other members of staff, suppliers and service users of the Council in the course of your employment or engagement. If so, the Council expects you to help meet its data protection obligations to those individuals. For example, you should be aware that they may also enjoy the rights set out in paragraph 10.1 above.

11.3 If you have access to personal information, you must:

11.3.1 only access the personal information that you have authority to access, and only for authorised purposes;

11.3.2 only allow other Council staff to access personal information if they have appropriate authorisation;

11.3.3 only allow individuals who are not Council staff to access personal information if you have specific authority to do so from the Clerk.

11.3.4 keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other precautions set out in the Council's information security policy;

11.3.5 not remove personal information, or devices containing personal information (or which can be used to access it), from the Council's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device; and

11.3.6 not store personal information on local drives or on personal devices that are used for work purposes**.**

11.4 You should contact the Clerk if you are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):

11.4.1 processing of personal data without a lawful basis for its processing or, in the case of sensitive personal information, without one of the conditions in paragraph 6.2.2 being met;
11.4.2 any data breach as set out in paragraph 14.1 below;
11.4.3 access to personal information without the proper authorisation;
11.4.4 personal information not kept or deleted securely;
11.4.5 removal of personal information, or devices containing personal information (or which can be used to access it), from the Council's premises without appropriate security measures being in place;
11.4.6 any other breach of this Policy or of any of the data protection principles set out in paragraph 4.1 above.

12 Information security

12.1 The Council will use appropriate technical and organisational measures to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. These may include:
12.1.1 making sure that, where possible, personal information is pseudonymised or encrypted;
12.1.2 ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
12.1.3 ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner; and
12.1.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

12.2 Where the Council uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. In particular, contracts with external organisations must provide that:
12.2.1 the organisation may act only on the written instructions of the Council;
12.2.2 those processing the data are subject to a duty of confidence;
12.2.3 appropriate measures are taken to ensure the security of processing;
12.2.4 sub-contractors are only engaged with the prior consent of the Council and under a written contract;
12.2.5 the organisation will assist the Council in providing subject access and allowing individuals to exercise their rights under the GDPR;
12.2.6 the organisation will assist the Council in meeting its GDPR obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;
12.2.7 the organisation will delete or return all personal information to the Council as requested at the end of the contract; and
12.2.8 the organisation will submit to audits and inspections, provide the Council with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the Council immediately if it is asked to do something infringing data protection law.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval of its terms by the Clerk.

13 Storage and retention of personal information

13.1 Personal information (and sensitive personal information) will be kept securely in accordance with the Council's information security policy.

13.2 Personal information (and sensitive personal information) should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances,

including the reasons why the personal information was obtained. Staff should follow the Council's records retention policy which set out the relevant retention period, or the criteria that should be used to determine the retention period. Where there is any uncertainty, staff should consult the Clerk.

13.3 Personal information (and sensitive personal information) that is no longer required will be deleted permanently from the Council's information systems and any hard copies will be destroyed securely.

14 Data breaches

14.1 A data breach may take many different forms, for example:

14.1.1 loss or theft of data or equipment on which personal information is stored;

14.1.2 unauthorised access to or use of personal information either by a member of staff or third party;

14.1.3 loss of data resulting from an equipment or systems (including hardware and software) failure;

14.1.4 human error, such as accidental deletion or alteration of data;

14.1.5 unforeseen circumstances, such as a fire or flood;

14.1.6 deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and

14.1.7 'blagging' offences, where information is obtained by deceiving the organisation which holds it.

14.2 The Council will:

14.2.1 make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and

14.2.2 notify the affected individuals, if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

15 International transfers

Any personal data transferred to countries or territories outside the European Economic Area ("EEA") will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union. Our website is also accessible from overseas so on occasion some personal data (for example in a newsletter) may be accessed from overseas.

16 Training

The Council will ensure that staff are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal information, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

17 Consequences of failing to comply

17.1 The Council takes compliance with this policy very seriously. Failure to comply with the policy:

17.1.1 puts at risk the individuals whose personal information is being processed; and

17.1.2 carries the risk of significant civil and criminal sanctions for the individual and the Council; and

17.1.3 may, in some circumstances, amount to a criminal offence by the individual.

17.2 Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under the Council's procedures, and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

17.3 If you have any questions or concerns about anything in this policy, do not hesitate to contact the Clerk.

WENDOVER PARISH COUNCIL
The Clock Tower, High Street, Wendover,
Aylesbury, Buckinghamshire HP22 6DU
Tel: 01296 623056 Email: clerk@wendover-pc.gov.uk

This policy was last updated in July 2023.

WENDOVER PARISH COUNCIL
The Clock Tower, High Street, Wendover,
Aylesbury, Buckinghamshire HP22 6DU
Tel: 01296 623056 Email: clerk@wendover-pc.gov.uk

Appendix A – General Privacy Notice

Your personal data – what is it?

"Personal data" is any information about a living individual which allows them to be identified from that data (for example a name, photographs, videos, email address, or address). Identification can be directly using the data itself or by combining it with other information which helps to identify a living individual (e.g., a list of staff may contain personnel ID numbers rather than names but if you use a separate list of the ID numbers which give the corresponding names to identify the staff in the first list then the first list will also be treated as personal data). The processing of personal data is governed by legislation relating to personal data which applies in the United Kingdom including the General Data Protection Regulation (the "GDPR) and other legislation relating to personal data and rights such as the Human Rights Act.

Who are we?

This Privacy Notice is provided to you by Wendover Parish Council which is the data controller for your data.
Other data controllers the Council works with are:

- Buckinghamshire Council
- Thames Valley Police
- Lloyds Bank

We may need to share your personal data we hold with them so that they can carry out their responsibilities to the Council. If we and the other data controllers listed above are processing your data jointly for the same purposes, then the council and the other data controllers may be "joint data controllers" which mean we are all collectively responsible to you for your data. Where each of the parties listed above are processing your data for their own independent purposes then each of us will be independently responsible to you and if you have any questions, wish to exercise any of your rights (see below) or wish to raise a complaint, you should do so directly to the relevant data controller.
A description of what personal data the Council processes and for what purposes is set out in this Privacy Notice.
The Council's Data Protection officer is the Clerk.

The Council will process some or all of the following personal data where necessary to perform its tasks:

- Names, titles, and aliases, photographs.
- Contact details such as telephone numbers, addresses, and email addresses.
- Where they are relevant to the services provided by a council, or where you provide them to us, we may process information such as gender, age, marital status, nationality,
- education/work history, academic/professional qualifications, hobbies, family composition, and dependents.
- Where you pay for activities, such as allotments, financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers.
- The information that we use may use some sensitive information such as ethnicity for the purposes of describing individuals

WENDOVER PARISH COUNCIL
The Clock Tower, High Street, Wendover,
Aylesbury, Buckinghamshire HP22 6DU
Tel: 01296 623056 Email: clerk@wendover-pc.gov.uk

How we use sensitive personal data

- We may process sensitive personal data including, as appropriate:
  - information about your physical or mental health or condition in order to monitor ability to access to our services
  - your racial or ethnic origin or religious or similar information in order to monitor usage of our services with regards to equal opportunities monitoring.
  - in order to comply with legal requirements and obligations to third parties such as for the prevention and detection of crime.
- These types of data are described in the GDPR as "Special categories of data" and require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal data.
- We may process special categories of personal data in the following circumstances:
  - In limited circumstances, with your explicit written consent.
  - Where we need to carry out our legal obligations.
  - Where it is needed in the public interest.
- Less commonly, we may process this type of personal data where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Do we need your consent to process your sensitive personal data?

- In limited circumstances, we may approach you for your written consent to allow us to process certain sensitive personal data. If we do so, we will provide you with full details of the personal data that we would like and the reason we need it, so that you can carefully consider whether you wish to consent.

The Council will comply with data protection law. This says that the personal data we hold about you must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept and destroyed securely including ensuring that appropriate technical and security measures are in place to protect your personal data to protect personal data from loss, misuse, unauthorised access and disclosure.

We use your personal data for some or all of the following purposes:

- To deliver public services including to understand your needs to provide the services that you request and to understand what we can do for you and inform you of other relevant services.
- To confirm your identity to provide some services.
- To contact you by post, email, telephone or using social media (e.g., Facebook, Twitter, WhatsApp).
- To help us to build up a picture of how we are performing.
- To prevent and detect fraud and corruption in the use of public funds and where necessary for the law enforcement functions.
- To enable us to meet all legal and statutory obligations and powers including any delegated functions.
- To carry out comprehensive safeguarding procedures (including due diligence and complaints handling) in accordance with best safeguarding practice from time to time with the aim of ensuring that all children and

WENDOVER PARISH COUNCIL
The Clock Tower, High Street, Wendover,
Aylesbury, Buckinghamshire HP22 6DU
Tel: 01296 623056 Email: clerk@wendover-pc.gov.uk

adults-at-risk are provided with safe environments and generally as necessary to protect individuals from harm or injury.
- To promote the interests of the council.
- To maintain our own accounts and records.
- To seek your views, opinions or comments.
- To notify you of changes to our facilities, services, events and staff, Councillors and other role holders.
- To send you communications which you have requested and that may be of interest to you. These may include information about campaigns, appeals, other new projects or initiatives.
- To process relevant financial transactions including grants and payments for goods and services supplied to the council
- To allow the statistical analysis of data so we can plan the provision of services.

Our processing may also include the use of CCTV systems for the prevention and prosecution of crime.

What is the legal basis for processing your personal data?

The Council is a public authority and has certain powers and obligations. Most of your personal data is processed for compliance with a legal obligation which includes the discharge of the council's statutory functions and powers. Sometimes when exercising these powers or duties it is necessary to process personal data of residents or people using the council's services. We will always take into account your interests and rights. This Privacy Notice sets out your rights and the council's obligations to you.
We may process personal data if it is necessary for the performance of a contract with you, or to take steps to enter into a contract. An example of this would be processing your data in connection with the use of sports facilities, or the acceptance of an allotment garden tenancy
Sometimes the use of your personal data requires your consent. We will first obtain your consent to that use.

Sharing your personal data

This section provides information about the third parties with whom the council may share your personal data. These third parties have an obligation to put in place appropriate security measures and will be responsible to you directly for the manner in which they process and protect your personal data. It is likely that we will need to share your data with some or all of the following (but only where necessary):
- The data controllers listed above under the heading "Other data controllers the council works with".
- Our agents, suppliers and contractors. For example, we may ask a commercial provider to publish or distribute newsletters on our behalf, or to maintain our database software.
- On occasion, other local authorities or not for profit bodies with which we are carrying out joint ventures e.g., in relation to facilities or events for the community.

How long do we keep your personal data?

We will keep some records permanently if we are legally required to do so. We may keep some other records for an extended period of time. For example, it is currently best practice to keep financial records for a minimum period of 8 years to support HMRC audits or provide tax information. We may have legal obligations to retain some data in connection with our statutory obligations as a public authority. The council is permitted to retain data in order to defend or pursue claims. In some cases, the law imposes a time limit for such claims (for example 3 years for personal injury claims or 6 years for contract claims). We will retain some personal data for this purpose as long as we believe it is necessary to be able to defend or pursue a claim. In general, we will endeavour to keep data only for as long as we need it. This means that we will delete it when it is no longer needed.

WENDOVER PARISH COUNCIL
The Clock Tower, High Street, Wendover,
Aylesbury, Buckinghamshire HP22 6DU
Tel: 01296 623056 Email: clerk@wendover-pc.gov.uk

Your rights and your personal data

You have the following rights with respect to your personal data:
When exercising any of the rights listed below, in order to process your request, we may need to verify your identity for your security. In such cases we will need you to respond with proof of your identity before you can exercise these rights.

1) The right to access personal data we hold on you

- At any point you can contact us to request the personal data we hold on you as well as why we have that personal data, who has access to the personal data and where we obtained the personal data from. Once we have received your request, we will respond within one month.
- There are no fees or charges for the first request but additional requests for the same personal data or requests which are manifestly unfounded or excessive may be subject to an administrative fee.

2) The right to correct and update the personal data we hold on you

- If the data we hold on you is out of date, incomplete or incorrect, you can inform us and your data will be updated.

3) The right to have your personal data erased

- If you feel that we should no longer be using your personal data or that we are unlawfully using your personal data, you can request that we erase the personal data we hold.
- When we receive your request, we will confirm whether the personal data has been deleted or the reason why it cannot be deleted (for example because we need it for to comply with a legal obligation).

4) The right to object to processing of your personal data or to restrict it to certain purposes only

- You have the right to request that we stop processing your personal data or ask us to restrict processing. Upon receiving the request, we will contact you and let you know if we are able to comply or if we have a legal obligation to continue to process your data.

5) The right to data portability

- You have the right to request that we transfer some of your data to another controller. We will comply with your request, where it is feasible to do so, within one month of receiving your request.

6) The right to withdraw your consent to the processing at any time for any processing of data to which consent was obtained

- You can withdraw your consent easily by telephone, email, or by post (see Contact Details below).

7) The right to lodge a complaint with the Information Commissioner's Office.

- You can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

Transfer of Data Abroad

Any personal data transferred to countries or territories outside the European Economic Area ("EEA") will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union. Our website is also accessible from overseas so on occasion some personal data (for example in a newsletter) may be accessed from overseas.

WENDOVER PARISH COUNCIL
The Clock Tower, High Street, Wendover,
Aylesbury, Buckinghamshire HP22 6DU
Tel: 01296 623056 Email: clerk@wendover-pc.gov.uk

Further processing

If we wish to use your personal data for a new purpose, not covered by this Privacy Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing.

Changes to this notice

We keep this Privacy Notice under regular review, and we will place any updates on the WPC website www.wendover-pc.gov.uk. This notice was last updated in July 2023.

Contact Details

Please contact us if you have any questions about this Privacy Notice or the personal data, we hold about you or to exercise all relevant rights, queries or complaints at:
The Clock Tower
High Street
Wendover
Bucks HP22 6DU
Email: clerk@wendover-pc.gov.uk

You can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

WENDOVER PARISH COUNCIL
The Clock Tower, High Street, Wendover,
Aylesbury, Buckinghamshire HP22 6DU
Tel: 01296 623056 Email: clerk@wendover-pc.gov.uk

Appendix B – Internal Privacy Notice

For staff*, Councillors and Role Holders**

*"Staff" means employees, workers, agency staff and those retained on a temporary or permanent basis
**Includes, volunteers, contractors, agents, and other role holders within the council including former staff*and former Councillors. This also includes applicants or candidates for any of these roles.

Your personal data – what is it?

"Personal data" is any information about a living individual which allows them to be identified from that data (for example a name, photograph, video, email address, or address). Identification can be directly using the data itself or by combining it with other information which helps to identify a living individual (e.g., a list of staff may contain personnel ID numbers rather than names but if you use a separate list of the ID numbers which give the corresponding names to identify the staff in the first list then the first list will also be treated as personal data). The processing of personal data is governed by legislation relating to personal data which applies in the United Kingdom including the General Data Protection Regulation (the "GDPR") and other legislation relating to personal data and rights such as the Human Rights Act.

Who are we?

This Privacy Notice is provided to you by Wendover Parish Council which is the data controller for your data.
The Council works together with the following data controllers:

- Buckinghamshire Council
- HMRC
- Pension providers -LGPS and Smart Pension
- Former and prospective employers (for references)
- DBS services suppliers where appropriate
- Payroll services providers – Numbers Ltd
- H&S and Training providers – Ellis Whittham (Worknest)
- Lloyds Bank

We may need to share personal data we hold with them so that they can carry out their responsibilities to the council and our community. The organisations referred to above will sometimes be "joint data controllers". This means we are all responsible to you for how we process your data where for example two or more data controllers are working together for a joint purpose. If there is no joint purpose or collaboration, then the data controllers will be independent and will be individually responsible to you.

The Council will comply with data protection law. This says that the personal data we hold about you must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept and destroyed securely including ensuring that appropriate technical and security measures are in place to protect your personal data to protect personal data from loss, misuse, unauthorised access and disclosure.

WENDOVER PARISH COUNCIL
The Clock Tower, High Street, Wendover,
Aylesbury, Buckinghamshire HP22 6DU
Tel: 01296 623056 Email: clerk@wendover-pc.gov.uk

What data do we process?

- Names, titles, and aliases, photographs.
- Start date / leaving date
- Contact details such as telephone numbers, addresses, and email addresses.
- Where they are relevant to our legal obligations, or where you provide them to us, we may process information such as gender, age, date of birth, marital status, nationality, education/work history, academic/professional qualifications, employment details, hobbies, family composition, and dependents.
- Non-financial identifiers such as passport numbers, driving licence numbers, vehicle registration numbers, taxpayer identification numbers, staff identification numbers, tax reference codes, and national insurance numbers.
- Financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers.
- Financial information such as National Insurance number, pay and pay records, tax code, tax and benefits contributions, expenses claimed.
- Other operational personal data created, obtained, or otherwise processed in the course of carrying out our activities, including but not limited to, CCTV footage, recordings of telephone conversations, IP addresses and website visit histories, logs of visitors, and logs of accidents, injuries and insurance claims.
- Next of kin and emergency contact information
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process and referral source (e.g., agency, staff referral))
- Location of employment or workplace.
- Other staff data (not covered above) including level, performance management information, languages and proficiency; licences/certificates, immigration status; employment status; information for disciplinary and grievance proceedings; and personal biographies.
- CCTV footage and other information obtained through electronic means such as swipecard records.
- Information about your use of our information and communications systems.

We use your personal data for some or all of the following purposes: -

Please note: We need all the categories of personal data in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations.

- Making a decision about your recruitment or appointment.
- Determining the terms on which you work for us.
- Checking you are legally entitled to work in the UK.
- Paying you and, if you are an employee, deducting tax and National Insurance contributions.
- Providing any contractual benefits to you
- Liaising with your pension provider.
- Administering the contract, we have entered into with you.
- Management and planning, including accounting and auditing.
- Conducting performance reviews, managing performance and determining performance requirements.
- Making decisions about salary reviews and compensation.
- Assessing qualifications for a particular job or task, including decisions about promotions.
- Conducting grievance or disciplinary proceedings.
- Making decisions about your continued employment or engagement.
- Making arrangements for the termination of our working relationship.

WENDOVER PARISH COUNCIL
The Clock Tower, High Street, Wendover,
Aylesbury, Buckinghamshire HP22 6DU
Tel: 01296 623056 Email: clerk@wendover-pc.gov.uk

- Education, training and development requirements.
- Dealing with legal disputes involving you, including accidents at work.
- Ascertaining your fitness to work.
- Managing sickness absence.
- Complying with health and safety obligations.
- To prevent fraud.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- To conduct data analytics studies to review and better understand employee retention and attrition rates.
- Equal opportunities monitoring.
- To undertake activity consistent with our statutory functions and powers including any delegated functions.
- To maintain our own accounts and records.
- To seek your views or comments.
- To process a job application.
- To administer councillors' interests
- To provide a reference.

Our processing may also include the use of CCTV systems for monitoring purposes.
Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal data.
We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

- Where we need to perform the contract, we have entered into with you.
- Where we need to comply with a legal obligation.

We may also use your personal data in the following situations, which are likely to be rare:
- Where we need to protect your interests (or someone else's interests).
- Where it is needed in the public interest [or for official purposes].

How we use sensitive personal data

- We may process sensitive personal data relating to staff, Councillors and role holders including, as appropriate:
  - information about your physical or mental health or condition in order to monitor sick leave and take decisions on your fitness for work.
  - your racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation.
  - in order to comply with legal requirements and obligations to third parties.
- These types of data are described in the GDPR as "Special categories of data" and require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal data.
- We may process special categories of personal data in the following circumstances:
  - In limited circumstances, with your explicit written consent.
  - Where we need to carry out our legal obligations.
  - Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our pension scheme.
  - Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.

WENDOVER PARISH COUNCIL
The Clock Tower, High Street, Wendover,
Aylesbury, Buckinghamshire HP22 6DU
Tel: 01296 623056 Email: clerk@wendover-pc.gov.uk

- Less commonly, we may process this type of personal data where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Do we need your consent to process your sensitive personal data?

- We do not need your consent if we use your sensitive personal data in accordance with our rights and obligations in the field of employment and social security law.
- In limited circumstances, we may approach you for your written consent to allow us to process certain sensitive personal data. If we do so, we will provide you with full details of the personal data that we would like and the reason we need it, so that you can carefully consider whether you wish to consent.
- You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Information about criminal convictions

- We may only use personal data relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided, we do so in line with our data protection policy.
- Less commonly, we may use personal data relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.
- Where appropriate, we will collect personal data about criminal convictions as part of the recruitment process or we may be notified of such personal data directly by you in the course of you working for us.

What is the legal basis for processing your personal data?

Some of our processing is necessary for compliance with a legal obligation.
We may also process data if it is necessary for the performance of a contract with you, or to take steps to enter into a contract.
We will also process your data in order to assist you in fulfilling your role in the council including administrative support or if processing is necessary for compliance with a legal obligation.

Sharing your personal data

Your personal data will only be shared with third parties including other data controllers where it is necessary for the performance of the data controllers' tasks or where you first give us your prior consent. It is likely that we will need to share your data with:

- Our agents, suppliers and contractors. For example, we ask Ellis Whittam to manage our HR functions and Numbers Ltd to manage our payroll functions.
- Other data controllers, such as local authorities, public authorities, central government and agencies such as HMRC, DVLA, Buckinghamshire Council.
- Staff pension providers – Buckinghamshire Council Local Government Pension Scheme and Smart Pensions
- The Council's banking institutions for the purposes of paying salaries and expenses
- Former and prospective employers
- DBS services suppliers
- Recruitment Agencies such as Adecco and Hays
- Credit reference agencies such as Equifax, Call Credit and Experian
- Professional advisors such as, Ellis Whittam and Parrott & Coales or another solicitor
- Trade unions or employee representatives such as the SLCC, ALCC, BALC or other employees

WENDOVER PARISH COUNCIL
The Clock Tower, High Street, Wendover,
Aylesbury, Buckinghamshire HP22 6DU
Tel: 01296 623056 Email: clerk@wendover-pc.gov.uk

How long do we keep your personal data?

We will keep some records permanently if we are legally required to do so. We may keep some other records for an extended period of time. For example, it is currently best practice to keep financial records for a minimum period of 8 years to support HMRC audits or provide tax information. We may have legal obligations to retain some data in connection with our statutory obligations as a public authority. The council is permitted to retain data in order to defend or pursue claims. In some cases, the law imposes a time limit for such claims (for example 3 years for personal injury claims or 6 years for contract claims). We will retain some personal data for this purpose as long as we believe it is necessary to be able to defend or pursue a claim. In general, we will endeavour to keep data only for as long as we need it. This means that we will delete it when it is no longer needed.

Your responsibilities

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your working relationship with us.

Your rights in connection with personal data

You have the following rights with respect to your personal data: -
When exercising any of the rights listed below, in order to process your request, we may need to verify your identity for your security. In such cases we will need you to respond with proof of your identity before you can exercise these rights.

11) The right to access personal data we hold on you

- At any point you can contact us to request the personal data we hold on you as well as why we have that personal data, who has access to the personal data and where we obtained the personal data from. Once we have received your request, we will respond within one month.
- There are no fees or charges for the first request but additional requests for the same personal data or requests which are manifestly unfounded or excessive may be subject to an administrative fee.

2) The right to correct and update the personal data we hold on you

- If the data we hold on you is out of date, incomplete or incorrect, you can inform us and your data will be updated.

3) The right to have your personal data erased

- If you feel that we should no longer be using your personal data or that we are unlawfully using your personal data, you can request that we erase the personal data we hold.
- When we receive your request, we will confirm whether the personal data has been deleted or the reason why it cannot be deleted (for example because we need it for to comply with a legal obligation).

4) The right to object to processing of your personal data or to restrict it to certain purposes only

- You have the right to request that we stop processing your personal data or ask us to restrict processing. Upon receiving the request, we will contact you and let you know if we are able to comply or if we have a legal obligation to continue to process your data.

5) The right to data portability

- You have the right to request that we transfer some of your data to another controller. We will comply with your request, where it is feasible to do so, within one month of receiving your request.

WENDOVER PARISH COUNCIL
The Clock Tower, High Street, Wendover,
Aylesbury, Buckinghamshire HP22 6DU
Tel: 01296 623056 Email: clerk@wendover-pc.gov.uk

6) The right to withdraw your consent to the processing at any time for any processing of data to which consent was obtained

- You can withdraw your consent easily by telephone, email, or by post (see Contact Details below).

7) The right to lodge a complaint with the Information Commissioner's Office.

- You can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

Transfer of Data Abroad

Any personal data transferred to countries or territories outside the European Economic Area ("EEA") will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union. Our website is also accessible from overseas so on occasion some personal data (for example in a newsletter) may be accessed from overseas.

Further processing

If we wish to use your personal data for a new purpose, not covered by this Privacy Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing, if we start to use your personal data for a purpose not mentioned in this notice.

Changes to this notice

We keep this Privacy Notice under regular review, and we will place any updates on the WPC website www.wendover-pc.gov.uk . This Notice was last updated in July 2023.

WENDOVER PARISH COUNCIL
The Clock Tower, High Street, Wendover,
Aylesbury, Buckinghamshire HP22 6DU
Tel: 01296 623056 Email: clerk@wendover-pc.gov.uk

Appendix C – DPIA Checklist

A. Under the GDPR, data protection impact assessments (DPIAs) are mandatory where the processing poses a high risk to the rights and freedoms of individuals. While they can also be carried out in other situations, councils need to be able to evaluate when a DPIA is required.

B. This checklist helps you make that assessment and provides a springboard for some of the issues you will need to consider in more detail if you do need to carry out a DPIA.

1. Do you need to carry out a DPIA?

(a) What is the objective/intended outcome of the project?

(b) Is it a significant piece of work affecting how services/operations are currently provided?

(c) Who is the audience or who will be affected by the project?

(d) Will the project involve the collection of new personal data about people? *(e.g. new identifiers or behavioural information relating to individuals?)*

(e) Will the project involve combining anonymised data sources in a way that may give rise to a risk that individuals could be identified?

(f) Will the project involve combining datasets originating from different processing operations or data controllers in a way which would exceed the reasonable expectations of the individuals?

(g) Is data being processed on a large scale?

(h) Will the project compel individuals to provide personal data about themselves?

(i) Will personal data about individuals be disclosed to organisations or people who have not previously had routine access to the personal data?

(j) Will personal data be transferred outside the EEA?

(k) Is personal data about individuals to be used for a purpose it is not currently used for, or in a way it is not currently used?

(l) Will personal data about children under 13 or other vulnerable persons be collected or otherwise processed?

(m) Will new technology be used which might be seen as privacy intrusive? (e.g. tracking, surveillance, observation or monitoring software, capture of image, video or audio or location)

(n) Is monitoring or tracking or profiling of individuals taking place?

(o) Is data being used for automated decision making with legal or similar significant effect?

(p) Is data being used for evaluation or scoring? (e.g. performance at work, economic situation, health, interests or behaviour)

(q) Is sensitive data being collected including:

(i) Race
(ii) Ethnic origin
(iii) Political opinions
(iv) Religious or philosophical beliefs
(v) Trade union membership
(vi) Genetic data
(vii) Biometric data (e.g. facial recognition, finger print data)
(viii) Health data

WENDOVER PARISH COUNCIL
The Clock Tower, High Street, Wendover,
Aylesbury, Buckinghamshire HP22 6DU
Tel: 01296 623056 Email: clerk@wendover-pc.gov.uk

(ix) Data about sex life or sexual orientation?

(r) Will the processing itself prevent data subjects from exercising a right or using a service or contract?

(s) Is the personal data about individuals of a kind likely to raise privacy concerns or is it personal data people would consider to be particularly private or confidential?

(t) Will the project require contact to be made with individuals in ways they may find intrusive?

2. Other issues to consider when carrying out a DPIA

(a) In addition to considering the above issues in greater detail, when conducting a DPIA, you will also need to look at issues including:

(i) The lawful grounds for processing and the capture of consent where appropriate

(ii) The purposes the data will be used for, how this will be communicated to the data subjects and the lawful grounds for processing

(iii) Who the data will be disclosed to

(iv) Where the data will be hosted and its geographical journey (including how data subjects will be kept informed about this)

(v) The internal process for risk assessment

(vi) Who needs to be consulted (DPO, data subjects, the Information Commissioners Office ("ICO"))

(vii) Data minimisation (including whether data can be anonymised)

(viii) How accuracy of data will be maintained

(ix) How long the data will be retained and what the processes are for deletion of data

(x) Data storage measures

(xi) Data security measures including what is appropriate relative to risk and whether measures such as encryption or pseudonymisation can be used to reduce risk

(xii) Opportunities for data subject to exercise their rights

(xiii) What staff or, as appropriate, councillor training is being undertaken to help minimise risk

(xiv) The technical and organisational measures used to reduce risk (including allowing different levels of access to data and red flagging unusual behaviour or incidents)

3. The GDPR requires that councils carry out a DPIA when processing is likely to result in a high risk to the rights and freedoms of data subjects. For a council, examples might include using CCTV to monitor public areas.

WENDOVER PARISH COUNCIL
The Clock Tower, High Street, Wendover,
Aylesbury, Buckinghamshire HP22 6DU
Tel: 01296 623056 Email: clerk@wendover-pc.gov.uk

4. If two or more of the following apply, it is likely that you will be required to carry out a DPIA. This does not apply to existing systems but would apply if you introduced a new system.

1. Profiling is in use. Example: you monitor website clicks or behaviour and record people's interests. ☐
2. Automated-decision making. Example: when processing leads to the potential exclusion of individuals. ☐
3. CCTV surveillance of public areas. Processing used to observe, monitor or control data subjects. ☐
4. Sensitive personal data as well as personal data relating to criminal convictions or offences. ☐
5. Large scale data processing. There is no definition of "large scale". However consider: the number of data subjects concerned, the volume of data and/or the range of different data items being processed. ☐
6. Linked databases - in other words, data aggregation. Example: two datasets merged together, that could "exceed the reasonable expectations of the user". E.g. you merge your mailing list with another council, club or association. ☐
7. Data concerning vulnerable data subjects, especially when power imbalances arise, e.g. staff-employer, where consent may be vague, data of children, mentally ill, asylum seekers, elderly, patients. ☐
8. "New technologies are in use". E.g. use of social media, etc. ☐
9. Data transfers outside of the EEA. ☐
10. "Unavoidable and unexpected processing". For example, processing performed on a public area that people passing by cannot avoid. Example: Wi-Fi tracking. ☐