Hartpury Parish Council

DATA PROTECTION POLICY

Adopted: 2nd March 2026

Reviewed and agreed: 4th May 2026

DATA PROTECTION

Purpose

The council is committed to being transparent about how it collects and uses the personal data, and to meeting our data protection obligations. This policy sets out the council's commitment to data protection, and your rights and obligations in relation to personal data in line with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018(DPA)

The Council is exempt from requiring a Data Protection Officer, however, has designated the Clerk as the person with responsibility for ensuring compliance with Data Protection within the Council. Any questions or requests should be directed to the Clerk who can be contacted by email parishclerk@hartpury-pc.gov.uk

The policy is applicable to all councillors and any employees, partners, voluntary groups, third parties and agents authorised by them.

The Council shall ensure that all users fully understand its obligations and have undertaken the necessary training to demonstrate compliance with this policy.

This policy applies to all personal information created or held by the Council, in all formats.

Definitions

"Personal data" is any information that relates to a living person who can be identified from that data (a 'data subject') on its own, or when taken together with other information. It includes both automated personal data and manual filing systems where personal data are accessible according to specific criteria. It does not include anonymised data.

"Processing" is any use that is made of data, including collecting, recording, organising,consulting, storing, amending, disclosing or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health,sex life or sexual orientation and genetic or biometric data as well as criminal convictions and offences.

Processing

The council will process your **personal data** (that is not classed as special categories of personal data) for one or more of the following reasons:

1) it is necessary for the performance of a contract, e.g., your contract of employment (or services);

2) it is necessary to comply with any legal obligation;

3) it is necessary for the council's legitimate interests (or for the legitimate interests of a third party), unless there is a good reason to protect your personal data which overrides those legitimate interests;

4) it is necessary to protect the vital interests of a data subject or another person;

5) it is necessary for the performance if a task carried out in the public interest or in the exercise of official authority vested in the controller.

If the council processes your personal data (excluding special categories of personal data) in line with one of the above bases, it does not require your consent. Otherwise, the council is required to gain your consent to process your personal data. If the council asks for your consent to process personal data, then we will explain the reason for the request. You do not need to consent or can withdraw consent later.

The council will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it. Personal data gathered during the employment is held in your personnel file in hard copy and electronic format on HR and IT systems and servers. The periods for which the council holds your HR-related personal data are contained in our privacy notices to individuals.

Sometimes the council will share your personal data with contractors and agents to carry out our obligations under a contract with the individual or for our legitimate interests. We require those individuals or companies to keep your personal data confidential and secure and to protect it in accordance with Data Protection law and our policies. They are only permitted to process that data for the lawful purpose for which it has been shared and in accordance withour instructions.

The council will update HR-related personal data promptly if you advise that your information has changed or is inaccurate. You may be required to provide documentary evidence in some circumstances.

The council keeps a record of our processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation(GDPR).

The council will only process **special categories of your personal data** (see above) on the following basis in accordance with legislation:

1) where it is necessary for carrying out rights and obligations under employment law or a collective agreement;
2) where it is necessary to protect your vital interests or those of another person whereyou are physically or legally incapable of giving consent;
3) where you have made the data public;
4) where it is necessary for the establishment, exercise or defence of legal claims;
5) where it is necessary for the purposes of occupational medicine or for the assessment of your working capacity;
6) where it is carried out by a not-for-profit body with a political, philosophical, religiousor trade union aim provided the processing relates to only members or former members provided there is no disclosure to a third party without consent;
7) where it is necessary for reasons for substantial public interest on the basis of law which is proportionate to the aim pursued and which contains appropriate safeguards;
8) where is it necessary for reasons of public interest in the area of public health;
9) where is it necessary for archiving purposes in the public interest or scientific and historical research purposes.

If the council processes special categories of your personal data in line with one of the above bases, it does not require your consent. In other cases, the council is required to gain your consent to process your special categories of personal data. If the council asks for your consent to process a special category of personal data, then we will explain the reason for the request. You do not have to consent or can withdraw consent later.

Some processing the Council carries out may result in risks to privacy, where processing would result in high risk to your rights the council will carry out a data protection impact assessment (DPIA) to determine the necessity and proportionality of processing. This will include considering the purposes for which it is carried out, the risks to the data subject, and any measures that can be taken to mitigate the risks.

Individual Rights

All data subjects have rights in relation to their personal data.

You have the right to make a Subject Access Request (SAR), a SAR will inform you what data is held, the reason, the retention period, and your right to erasure. You can be provided with a copy of your personal data that is being processed, usually electronically, unless otherwise agreed. Additional paper copies may be charged a fee for administrative costs.

To make a SAR please address the request to the clerk of the council. In some cases, proof of ID may be required, in these cases the Council will inform you and let you know what documentation is required. The Council will respond to a SAR within one calendar month of receiving the request, in the case that there is a large amount of data that will not be possible to achieve within one month the Council will inform you of this in writing.

Other rights include requiring the Council to:

1) rectify inaccurate data
2) stop processing or erase data that is no longer necessary
3) stop processing or erase data if your interests override the Council's legitimate grounds for processing data (where the Council relies on legitimate interests as the reason for processing)
4) stop processing or erase data if processing is unlawful
5) stop processing data for a period of time if the data is inaccurate or if there is a dispute over processing the data as per point 3 above
6) complain to the information commissioner. You can do this by contacting their office directly, full contact details can be found on their website (www.ico.org.uk).

To request that any of these steps are taken please contact the Clerk of the Council.

Data Security and Breaches

The Council takes the security of personal data seriously and has controls in place to protect against loss, accidental destruction, misuse or disclosure and to ensure that data is not accessed except by staff completing their duties.

In some cases the Council may engage a third party to process data on our behalf, such parties do so on the basis of written instruction, are bound by confidentiality and are obliged to implement appropriate measure to ensure that data is secure.

The Council will not share personal data unless required to so so by law or in the case that it is in the best interests of the data subject or when failure to share may carry risk to vunerable groups/individuals. Information must always be shared in a secure and appropriate manner and in accordance with the information type. The Council will be transparent and as open as possible about how and with whom data is shared; with what authority; and for what purpose; and with what protections and safeguards.

The Council has measures in place to minimise and prevent data breaches from happening. Should a breach occur the Council must take notes and keep evidence of that breach.

All users have an obligation to report actual or potential data protection compliance failures as soon as possible and take immediate steps to minimise the impact and to assist with managing risk. The Council will fully investigate both actual and potential failures and take remedial steps if necessary maintain a register of compliance failures. If the incident involves or impacts personal data it must be reported to the ICO within 72 hours.

If the breach is likely to result in high risk to data subjects they will be informed and informed of likely consequences and mitigation measures that have been taken.

Individual Responsibilities

Data subjects are responsible for helping to keep personal data updated. If data provided to the Council changes such as moving house or changing bank accounts, you should inform the Council.

If you have access to personal data during the course of your work with the Council you have a responsibility to help meet data protection obligations and abide by this policy. Whilst you have access to personal data the following is required:

1) only access data you have the authority for and only for authorsied purposes
2) do not disclose any data to individuals without proper authorisation
3) keep data secure (e.g locking computers/devices when not actively in use, locking filing cabinets, not leaving documents on desks)
4) do not store personal data on local drives or personal devices that are used for work purposes (use of own devices covered under the Council's IT Policy)
5) never transfer personal data outside of the European Economic Area except in compliance with the law and with authorisation from the Council
6) ask for help from the Council's data protection lead (the Clerk) if unsure about data protection, if you notice a potential breach or any areas of data security that could be improved.

Failure to comply with these requirements may amount to a disciplinary offence and will be dealt with under the Council's disciplinary procedure. Significant or deliberate breaches of this policy may constitute gross misconduct and result in dismissal without notice. For Councillors this may result in a breach of the Code of Conduct and be referred to the monitoring officer.

Records Management

It is necessary for the Council to retain a number of data sets as part of managing council business, these often contain personal data. The Council shall retain records as per the Document Retention and Record Management Policy.