

Inventory of Personal Data Captured, Stored and Processed by Gt Witchingham Parish Council

Category	Personal detail held	Purpose	How held	Legal basis for processing	With whom do we share this data
Personel - Clerk to the Council					
Contract	Terms of employment	Contractual	Electronically/Hard copy	Legal obligation	
Payroll/Pension	Address, NI no, Tax Code,	Legislative	Electronically		HMRC, payroll provider, Pension Provider
Salary claims	Bank details	Financial	Electronically/Hard copy		Bank
Timesheets	Hours and record of work	Contractual/Audit	Electronically		
Appraisal	Performance & development	Contractual	Electronically		
Public Contact (List)	Address, email, tel no	Public reference	Electronically/Hard copy	Public Task	Public
Councillors					
Register of Interests	Disclosable pecuniary & other interests	Democracy	Hard Copy	Legal obligation	This is Public Knowledge
Contact information	Name, address, email, tel no	Communication	Electronically/Hard copy	Public Task	Names public knowledge.
Public Contact (List)	Name, email, tel no	Public Reference	Electronically/Hard copy	Consent	Public
Contractors /Suppliers where we hold personal data of a natural person (not the data of a limited company or of another council)					
Quotes/Invoices	Name, address, email, tel no, bank details	Business/Financial	Electronically/Hard copy	Contract	Public exercise of rights - inspection on audit
Residents					
Electoral Register	Name, address	Legislative	Hard Copy	Public Task	Public Document required by law, GWPC choose to hold.
Members of public					
Enquiries	Name, address email, tel no	Democracy	Electronically/Hard copy	Public Task	
Volunteers					
Play Area Working Party	Name, address, email, tel no	Communication	Electronically/Hard copy	Public Task	Names public knowledge, other data is confidential

GREAT WITCHINGHAM PARISH COUNCIL

PRIVACY STATEMENT

Great Witchingham Parish Council (the Council) is the data controller and the Clerk to the Council is the data processor. Contact details for the Clerk are

Mrs Patricia Kirby

128 Fakenham Road

Taverham NR8 6QH

Telephone number: 01603 860671 (answer machine)

email address: greatwitchinghamparishcouncil@gmail.com

When you contact us

The information you provide (personal information such as name, address, email address, phone number, organisation) will be processed and stored to enable us to contact you and respond to your correspondence, provide information and/or access our facilities and services. Your personal information will be not shared or provided to any other third party.

The Councils Right to Process Information

General Data Protection Regulation Article 6 (1) (a) (b) (c) & (e) sets out the legal basis for processing data

- a Consent - Processing is with consent of the data subject
- b Contract - Processing is necessary for the performance of a contract
- c Legal obligation - Processing is necessary for compliance with a legal obligation or
- e Public Task - Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

Information Security

The Council has a duty to ensure the security of personal data. We make sure that your information is protected from unauthorised access, loss, manipulation, falsification, destruction or unauthorised disclosure. This is done through appropriate technical measures and working practices.

We will only keep your data for the purpose it was collected for and only for as long as is necessary. After which it will be deleted. (You may request the deletion of your data held by the Council at any time).

Children

We will not process any data relating to a child (under 13) without the express parental/ guardian consent of the child concerned.

Access to Information

You have the right to request access to the information we have on you. You can do this by contacting the data controller via the Parish Clerk. (Details as above)

Information Correction

If you believe that the information we have about you is incorrect, you may contact us so that we can update it and keep your data accurate. Please contact the data controller via the Parish Clerk to request this.

Information Deletion

If you wish the Council to delete the information about you please contact the data controller via the Parish Clerk to request this.

Right to Object

If you believe that your data is not being processed for the purpose it has been collected for, you may object: Please contact the data controller via the Parish Clerk to object.

Rights Related to Automated Decision Making and Profiling

The Council does not use any form of automated decision making or the profiling of individual personal data.

Conclusion: In accordance with the law, we only collect a limited amount of information about you that is necessary for correspondence, information and service provision. We do not use profiling, we do not sell or pass your data to third parties. We do not use your data for purposes other than those specified. We make sure your data is stored securely. We delete all information deemed to be no longer necessary.

We may update this statement periodically to reflect changes in the law and/or privacy practices.

Complaints

If you have a complaint regarding the way your personal data has been processed you may make a complaint to the data controller via the Parish Clerk and the Information Commissioners Office casework@ico.org.uk Tel: 0303 123 1113

GREAT WITCHINGHAM PARISH COUNCIL

GENERAL DATA PROTECTION REGULATION POLICY

Purpose of the policy and background to the General Data Protection Regulation

This policy explains to councillors, staff and the public about GDPR. Personal data must be processed lawfully, fairly and transparently; collected for specified, explicit and legitimate purposes; be adequate, relevant and limited to what is necessary for processing; be accurate and kept up to date; be kept only for as long as is necessary for processing and be processed in a manner that ensures its security. This policy updates any previous data protection policy and procedures to include the additional requirements of GDPR which apply in the UK from May 2018. The Government have confirmed that despite the UK leaving the EU, GDPR will still be a legal requirement.

This policy explains the duties and responsibilities of the council and it identifies the means by which the council will meet its obligations.

Identifying the roles and minimising risk

GDPR requires that everyone within the council must understand the implications of GDPR and that roles and duties must be assigned. The Council is the data controller and the Clerk is the Data Processor. It is the Clerk's duty to undertake an information audit and to manage the information collected by the council, the issuing of privacy statements, dealing with requests and complaints raised and also the safe disposal of information.

GDPR requires continued care by everyone within the council, councillors and staff, in the sharing of information about individuals, whether as a hard copy or electronically. A breach of the regulations could result in the council facing a fine from the Information Commissioner's Office (ICO) for the breach itself and also to compensate the individual(s) who could be adversely affected. Therefore, the handling of information is seen as high / medium risk to the council (both financially and reputationally) and one which must be included in the Risk Management Policy of the council. Such risk can be minimised by undertaking an information audit, issuing privacy statements, maintaining privacy impact assessments (an audit of potential data protection risks with new projects), minimising who holds data protected information and the council undertaking training in data protection awareness.

Data breaches

The Clerk will investigate breaches. Personal data breaches should be reported to the Clerk for investigation. The Clerk will conduct this with the support of the Chairman of the Council. Investigations must be undertaken within one month of the report of a breach. Procedures are in place to detect, report and investigate a personal data breach. The ICO will be advised of a breach (within 3 days) where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality, or any other significant economic or social disadvantage. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the Clerk will also have to notify those concerned directly.

It is unacceptable for non-authorised users to access IT using employees' log-in passwords or to use equipment while logged on. It is unacceptable for employees, volunteers and members to use IT in any way that may cause problems for the Council, for example the discussion of internal council matters on social media sites could result in reputational damage for the Council and to individuals.

Privacy Notices

Being transparent and providing accessible information to individuals about how the Council uses personal data is a key element of the Data Protection Act 2018 (DPA) and the EU General Data Protection Regulation (GDPR). The most common way to provide this information is in a privacy notice. This is a notice to inform individuals about what a council does with their personal information. A privacy notice will contain the name and contact details of the data controller, the purpose for which the information is to be used and the length of time for its use. It should be written clearly and should advise the individual that they can, at any time, withdraw their agreement for the use of this information. Issuing of a privacy notice must be detailed on the Information Audit kept by the council. The council will adopt a privacy notice to use, although some changes could be needed depending on the situation, for example where children are involved. All privacy notices must be verifiable.

Information Audit

The Clerk must undertake an information audit which details the personal data held, where it came from, the purpose for holding that information and with whom the council will share that information. This will include information held electronically or as a hard copy. Information held could change from year to year with different activities, and so the information audit will be reviewed at least annually or when the council undertakes a new activity. The information audit review should be conducted ahead of the review of this policy and the reviews should be minuted.

Individuals' Rights

GDPR gives individuals rights with some enhancements to those rights already in place:

- the right to be informed
- the right of access
- the right to rectification
- the right to erasure
- the right to restrict processing
- right to data portability
- the right to object
- the right not to be subject to automated decision-making including profiling.

The two enhancements of GDPR are that individuals now have a right to have their personal data erased (sometime known as the 'right to be forgotten') where their personal data is no longer necessary in relation to the purpose for which it was originally collected and data portability must be done free of charge. Data portability refers to the ability to move, copy or transfer data easily between different computers.

If a request is received to delete information, then the Clerk must respond to this request within a month. The Clerk has the delegated authority from the Council to delete information.

If a request is considered to be manifestly unfounded then the request could be refused or a charge may apply. The charge will be as detailed in the Council's Freedom of Information Publication Scheme. The Chairman of the Council will be informed of such requests.

Children

There is special protection for the personal data of a child. The age when a child can give their own consent is 13. If the council requires consent from young people under 13, the council must obtain a parent or guardian's consent in order to process the personal data lawfully. Consent forms for children age 13 plus, must be written in language that they will understand.

Summary

The main actions arising from this policy are:

- The Council must be registered with the ICO.
- A copy of this policy will be available on the Council's website. The policy will be considered as a core policy for the Council.
- An information audit will be conducted and reviewed at least annually or when projects and services change.
- Privacy notices must be issued.
- Data Protection will be included on the Council's Risk Management Policy.

All employees, volunteers and councillors are expected to comply with this policy at all times to protect privacy, confidentiality and the interests of the Council.

This policy document is written with current information and advice. It will be reviewed at least annually or when further advice is issued by the ICO.