Whitmore Parish Council (Borough of Newcastle under Lyme) General Data Protection Regulation (GDPR) and Data Policies May 2018

Whitmore Parish Council (WPC) may collect and use personal information about staff, councillors and other individuals who come into contact with the Council. This information is gathered in order to enable it to provide its statutory and other associated duties. Other than staff data that is required by law, WPC does not collect personal information other than contact details on a list server that individuals have given their consent for such use. The list server is a cloud-based service governed by UK and EU law.

Whitmore Parish Council may collect and process data as an official authority, with discretionary powers and these are set down in law. Currently, WPC does not process data.

Parishes have a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website. Parishes also have a duty to issue a Fair Processing Notice to all residents, this summarises the information held, why it is held and the other parties to whom it may be passed to. Whitmore Parish Council is registered with the ICO (https://ico.org.uk/ESDWebPages/Entry/Z866249X).

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 1998, and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically. On 25 May 2018 the Data Protection Act 1998 will be replaced by The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679). This EU law will be enshrined as UK law as part of Brexit.

All staff and Councillors involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held.

The Data Protection Act 1998 establishes eight enforceable principles that must be adhered to at all times:

1. Personal data shall be processed fairly and lawfully;
2. Personal data shall be obtained only for one or more specified and lawful purposes;
3. Personal data shall be adequate, relevant and not excessive;
4. Personal data shall be accurate and where necessary, 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 processed in accordance with the rights of data subjects under the Data Protection Act 1998;
7. Personal data shall be kept secure i.e. protected by an appropriate degree of security;
8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

WPC is committed to maintaining the above principles at all times. WPC will:

- Inform individuals why the information is being collected when it is collected;
- Inform individuals when their information is shared, and why and with whom it was shared;
- 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 the duty to respond to requests for access to personal information, known as Subject Access Requests; &
- Ensure our staff are aware of and understand our policies and procedures.

Complaints will be dealt with in accordance with the WPC complaints policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator). This policy will be reviewed as it is deemed appropriate, but no less frequently than every two years. The policy review will be undertaken by a designated Councillor. If you have any enquires in relation to this policy, please contact the Clerk to the Council who will also act as the contact point for any subject access requests.

Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk.

General Data Protection Regulations (GDPR)

Under the GDPR, the data protection principles set out the main responsibilities for organisations.

Article 5 of the GDPR requires that personal data shall be:

"a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to

implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

Article 5(2) requires that:

"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

GDPR Principals

- The regulation stipulates that anyone councils hold information on must give their explicit and 'informed' consent for their data to be retained for a set period of time and processed, which means the individual must be made aware of how their information is protected, what it's used for, and what the risks are. The Appendices sets out how we process data and how long we keep it for.
- GDPR makes organisations responsible for giving people clear and adequate information about how their information will be protected.
- Under GDPR people have more power to withdraw their consent and get their data amended or deleted. In other words, they have the 'right to be forgotten'.
- GDPR gives individuals the right to make a subject access request at any time and get a response within one month.
- During any cleansing operation (such as that caused by a Right to be Forgotten request) it will not be possible to delete some of those records. This might be for reasons of financial regulatory compliance, or for a number of other reasons where organisations can show they have 'legitimate' reason for retaining and processing the data. GDPR recommends that you will need to pseudonymise or anonymise the data you can't legitimately delete to be compliant.
- GDPR does not require Parish Councils to appoint a Data Protection Officer (DPO) to achieve compliance but parishes can do so or appoint a Councillor to oversee data. GDPR specifies that DPOs are responsible for activities including monitoring compliance, educating staff on their responsibilities, providing advice on privacy impact assessments and co-operating wherever necessary with the relevant supervisory authority. Parish Councils are now exempt from DPO requirements.
- GDPR is also going affect councils' relationships with IT suppliers. This is because by enhancing the rights of data subjects, GDPR not only increases the responsibilities for data 'controllers' (i.e. WPC), but also for data processors (i.e. your IT service provider or cloud provider). Both controllers and processors are under a similar duty to ensure that the regulations are properly implemented. Contracts will need to be reviewed so that both parties comply with the regulations.

What's new under the GDPR?

The public task basis in Article 6(1)(e) may appear new, but it is similar to the old condition for processing for functions of a public nature in Schedule 2 of the Data Protection Act 1998.

One key difference is that the GDPR says that the relevant task or function must have a clear basis in law.

The GDPR is also clear that public authorities can no longer rely on legitimate interests for processing carried out in performance of their tasks. In the past, some of this type of processing may have been done on the basis of legitimate interests. If you are a public authority, this means you may now need to consider the public task basis for more of your processing.

The GDPR also brings in new accountability requirements. You should document your lawful basis so that you can demonstrate that it applies. In particular, you should be able to identify a clear basis in either statute or common law for the relevant task, function or power for which you are using the personal data.

You must also update your privacy notice to include your lawful basis, and communicate this to individuals.

What is the 'public task' basis?

Article 6(1)(e) gives you a lawful basis for processing where:

"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"

This can apply if you are either:

- carrying out a specific task in the public interest which is laid down by law; or
- exercising official authority (for example, a public body's tasks, functions, duties or powers) which is laid down by law.

If you can show you are exercising official authority, including use of discretionary powers, there is no additional public interest test. However, you must be able to demonstrate that the processing is 'necessary' for that purpose.

'Necessary' means that the processing must be a targeted and proportionate way of achieving your purpose. You do not have a lawful basis for processing if there is another reasonable and less intrusive way to achieve the same result.

In this guide we use the term 'public task' to help describe and label this lawful basis. However, this is not a term used in the GDPR itself. Your focus should be on demonstrating either that you are carrying out a task in the public interest, or that you are exercising official authority.

In particular, there is no direct link to the concept of 'public task' in the Re-use of Public Sector Information Regulations 2015 (RPSI). There is some overlap, as a public sector body's core role and functions for RPSI purposes may be a useful starting point in demonstrating official authority for these purposes. However, you shouldn't assume that it is an identical test.

Appendix 1

WPC Procedures for responding to subject access requests made under the Data Protection Act 1998. Under the Data Protection Act 1998 any individual has the right to make a request to access the personal information held about them.

Requests for information must be made in writing; which includes email, and be addressed to the Clerk. If the initial request does not clearly identify the information required, then further enquiries will be made. The identity of the requestor must be established before the disclosure of any information. Evidence of identity can be established by requesting production of: a valid passport or photo driving licence and a utility bill with the current address.

WPC may make a charge of £10 for the provision of information.

The response time for subject access requests (under GDPR), once officially received, is one calendar month. However the month will not commence until after receipt of fees or clarification of information sought.

The Data Protection Act 1998 allows exemptions as to the provision of some information; therefore all information will be reviewed prior to disclosure.

Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another administration (e.g. borough, county or central government). Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the month statutory timescale.

Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail must be used.

Complaints about the above procedures should be made to the Chair of the Parish Council who will decide whether it is appropriate for the complaint to be dealt with in accordance with the WPC's complaint procedure. Complaints which are not appropriate to be dealt with through the WPC's complaint procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

Appendix 2

Data that Whitmore Parish Council might hold & retention policies:

- Minutes of meetings: are published on the website and are usually available for a year or alternatively are available from the Clerk. Minutes are kept indefiniteley.
- Financial information: is published on the website and is usually available for a year or alternatively is available from the Clerk for up to 7 years. Records are deleted after 7 years.

- Staff information: is only available to the individuals concerned and the current Chair and Vice Chair of the Parish Council. Records are deleted after 7 years. Pension information is held by the pension provider.
- Publicly Available Information: may be re-published on the Parish website but such information as government instructions; precepts; etc are not the responsibility of WPC.
- Publicly Available Information: published by WPC; e.g. standing orders; will be available on the WPC Website or in writing from the Clerk for the relevant period such documents cover.
- Neighbourhood Plan: WPC website provides a link to the Neighbourhood Development Plan website where all information is published. The NDP does not hold personal data.
- Correspondence (electronic, voice and paper): Anonymous correspondence is destroyed immediately without any action or record being kept. All letters, calls and emails from residents or external bodies are logged, responded to (within 10 working days) and deleted between 2 and 3 years. Any action taken will be informed to the enquirer by the relevant Councillor or Parish Clerk. Correspondence which is topic-specific; e.g. planning; roads; sewerage; traffic calming; HS2; etc is not considered personal data and will be kept for the duration of the topic, which might be many years.
- Correspondence that is forwarded to another body will be forwarded in its entirety and those requesting action where WPC must involve or inform a third party will be informed that their request has been forwarded. Email addresses that are not relevant to the request will be deleted.
- Correspondence that is an enquiry from a Resident but marked Confidential or some other soubriquet will not be forwarded to external bodies without the permission of the sender.
- Under GDPR residents will have to sign up to various topics by using the list server on the new website. Normally the magazine is delivered to the Occupier at each address in the Parish. Request for extra paper copies of the magazine will be required in writing/email.