EAST WITTERING & BRACKLESHAM

PARISH COUNCIL BREACH NOTIFICATION POLICY

1. SCOPE

1.1. This procedure applies in the event of a personal data breach under Article 33 Notification of a personal data breach to the supervisory authority, and Article 34 Communication of a personal data breach to the data subject of the GDPR.

1.2. The GDPR draws a distinction between a 'data controller' and a 'data processor' in order to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility. Therefore, each organisation, should establish whether it is data controller, or a data processor for the same data processing activity; it must be one or the other.

2. RESPONSIBILITY

2.1. All users (whether Employees/Staff, contractors or temporary Employees/Staff and third-party users) and Councillors of East Wittering & Bracklesham Parish Council are required to be aware of, and to follow this procedure in the event of a personal data breach.

3. PROCEDURE – BREACH NOTIFICATION DATA PROCESSOR TO DATA CONTROLLER

3.1. East Wittering & Bracklesham Parish Council shall report any personal data breach to the data controller (Clerk) without undue delay who will pass details to the Data Protection Officer. (GDPR-Info Ltd)

3.2. GDPR-*info* Ltd notifies their contact within the data controller, which is recorded in the Internal Breach Register.

3.3. Notification is made by [email, phone call, etc.].

3.4. Confirmation of receipt of this information is made by email

4. PROCEDURE – BREACH NOTIFICATION DATA CONTROLLER TO SUPERVISORY AUTHORITY

4.1. GDPR-Info Ltd shall notify the supervisory authority [ICO] without undue delay, of a personal data breach.

4.2. 4.1 GDPR-Info Ltd assesses whether the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach.

4.3. If a risk to the aforementioned is likely, GDPR-Info Ltd shall report any personal data breach to the supervisory authority without undue delay, and where feasible not later than 72 hours. Where data breach notification to the supervisory authority is not made within 72 hours, it shall be accompanied by the reasons for the delay.

4.4. The data controller (Clerk) shall provide the following information to the supervisory authority on a Breach Notification Form:

4.5. A description of the nature of the breach

4.6. The categories of personal data affected

4.7. Approximate number of data subjects affected

4.8. Approximate number of personal data records affected

4.9. Name and contact details of GDPR-*info* Ltd

4.10. Likely consequences of the breach

4.11. Any measures that have been or will be taken to address the breach, including mitigation

4.12. The information relating to the data breach, which may be provided in phases.

4.13. GDPR-*info* Ltd notifies their contact within the supervisory authority, which is recorded in the Internal Breach Register

4.14. Notification is made by [email, phone call, etc.].

4.15. Confirmation of receipt of this information is made by email.

5. PROCEDURE – BREACH NOTIFICATION DATA CONTROLLER TO DATA SUBJECT

5.1. Where the personal data breach is likely to result in high risk to the rights and freedoms of the data subject East Wittering & Bracklesham Parish Council shall notify the affected data subjects without undue delay, [using this form/in accordance with GDPR-*info* Ltd.'s recommendations].

5.2. The notification to the data subject shall describe in clear and plain language the nature of the breach including the information specified 4.4 above.

5.3. Appropriate measures have been taken to render the personal data unusable to any person who is not authorised to access it, such as encryption.

5.4. The controller has taken subsequent measure to ensure that the rights and freedoms of the data subjects are no longer likely to materialise.

5.5. It would require a disproportionate amount of effort. In such a scenario, there shall be a public communication or similar measure whereby the data subject is informed in an equally effective manner.

5.6. The supervisory authority may where it considers the likelihood of a personal data breach resulting in high risk require the data controller to communicate the personal data breach to the data subject.

East Wittering & Bracklesham Parish Council

Data Retention and Disposal Policy

1 Introduction

1.1 The guidelines set out in this document supports the Council's Data Protection Policy and assists us in compliance with the Freedom of Information Act 2000, the General Data Protection Regulation & The Data Protection Act 2018 and other associated legislation.

1.2 It is important that the Council has in place arrangements for the retention and disposal of documents necessary for the adequate management of services in undertaking its responsibilities. This policy sets out the minimum requirements for the retention of documents and sets out the requirements for the disposal of documents. However it is important to note that this is a live document and will be updated on a regular basis.

1.3 The Council will ensure that information is not kept for longer than is necessary and will retain the minimum amount of information that it requires to carry out its functions and the provision of services, whilst adhering to any legal or statutory requirements.

2 Aims and Objectives

2.1 It is recognised that up to date, reliable and accurate information is a vital to support the work that the Council do and the services that it provides to its residents. This document will help us to:-

- Ensure the retention and availability of the minimum amount of relevant information that is necessary for the Council to operate and provide services to the public.
- Comply with legal and regulatory requirements, including the Freedom of Information Act 2000, the Data Protection Act 1998, the General Data Protection Regulation, the Data Protection Act 2018 and the Environmental Information Regulations 2004.
- Save employees' time and effort when retrieving information by reducing the amount of information that may be held unnecessarily. This will assist them as they carry out their daily duties, or if searching for information requested under the Freedom of Information Act.
- Ensure archival records that are of historical value are appropriately retained for the benefit of future generations.

3 Scope

3.1 For the purpose of this Strategy, 'documents' includes electronic, microfilm, microfiche and paper records.

3.2 Where storage is by means of paper records, originals rather than photocopies should be retained where possible. **4 Standards**

4.1 The Council will make every effort to ensure that it meets the following standards of good practice:

- Adhere to legal requirements for the retention of information as specified in the Retention Schedule at Annex A. This document provides a framework for good practice requirements for retaining information.
- Personal information will be retained in locked filing cabinets within the Clerk's Office and/or the Senior Assistant's office, access to these documents will only be by authorised personnel.
- Disclosure information will be retained in a locked cabinet in the Clerk's Office.

- Appropriately dispose of information that is no longer required.
- Appropriate measures will be taken to ensure that confidential and sensitive information is securely destroyed.
- Information about unidentifiable individuals is permitted to be held indefinitely for historical, statistical or research purposes e.g. Equalities data.
- Wherever possible only one copy of any personal information will be retained and that will be held within the Clerk's Office or the Senior Assistant's Office.

5 Breach of Policy and Standards

5.1 Any employee who knowingly or recklessly contravenes any instruction contained in, or following from, this Policy and Standards may, depending on the circumstances of the case, have disciplinary action, which could include dismissal, taken against them.

6 Roles and Responsibilities

6.1 The Clerk has overall responsibility for the policy.

6.2 The Clerk is responsible for the maintenance and operation of this policy including ad-hoc checks to ensure compliance.

6.2 Other delegated staff are responsible for ensuring their records are kept and destroyed in line with this policy.

6.3 The Clerk responsible for ensuring that the guidelines set out in this policy are adhered to and to ensure that any documents disposed of are done so in accordance with their 'sensitivity' (i.e. whether they are normal waste or 'Confidential Waste'

7 Confidential Waste

7.1 Fundamentally any information that is required to be produced under the Freedom of Information Act or Environmental Information Regulations, is available on the website or is open to public inspection should NOT be treated as confidential waste.

7.2 However, any information that is protected by the Data Protection Act or as Confidential under the Councils Constitution should be treated as confidential waste for disposal purposes.

7.3 Examples of what constitutes confidential waste:

- Exempt information contained within committee reports.
- Files containing the personal details of an individual and files that predominantly relate to a particular individual or their circumstances. For example completed application forms and letters.
- Materials given to us on a 'confidential' or on a limited use basis e.g. material provided by contractors or the police.

7.4 Examples of what does not constitute confidential waste:

- Documents that are available to the public via our web site or by submitting an appropriate search request to ourselves for general information.
- All reports and background papers of matters taken to Committee in public session unless specifically exempt

8 Disposal of Documentation

8.1 Confidential waste which clearly shows any personal information or information which can be identified using the parameters set out in 7.3 will be shredded within the council buildings.

9 Retention

9.1 Timeframes for retention of documents have been set using legislative requirements and the Chartered Institute of Personnel and Professional Development (CIPD) guidelines.

9.2 Throughout retention the conditions regarding safe storage and controlled access will remain in place.

9.3 Disclosure information appertaining to Disclosure and Barring Checks must be kept securely in a locked cabinet. Only those entitled to see it in the course of their duties should have access. The security and confidentiality of all Disclosure information is closely registered under the Police Act 1997.

9.4 Disclosure information must not be retained for a period of more than six months and must be destroyed in a secure manner using the shredder in the Reception office.

9.5 Any unauthorised employee accessing or attempting to access Disclosures or Disclosure information or personnel records will be dealt with under the Council's disciplinary procedures.

9.6 The attached 'Appendix' shows the minimum requirements for the retention of documents as determined by those officers responsible for the management of these particular documentation types. Officers holding documents should exercise judgement as to whether they can be disposed of at the end of those periods detailed in the attached 'Appendix'

10 Storage and Access

10.1 Disclosure information is kept separately from personnel files and in securely lockable, nonportable cabinet with access strictly controlled and limited to the Clerk, and/or the Senior Assistant.

11 Handling

11.1 The Council complies with s124 of the Police Act 1997, so that Disclosure Information is only passed to those who are authorised to receive it in the course of their duties. The Council maintains a record of all those to who Disclosures or Disclosure Information has been revealed and recognises that it is a criminal offence to pass this information to anyone who is not entitled to receive it.

11.2 Personal information will only be available to those who are authorised officers.

11.3 Customers details and information will be kept up to date and reviewed annually by an authorised officer.

12 Usage

12.1 Disclosure information is only used for the specific purpose for which it was requested and for which the applicant's/employee's consent has been given. Disclosure Information will be shared between different areas of the Council, if necessary.

12.2 Where Disclosure information is shared with anyone other than the Clerk, the Senior Assistant and the direct Manager the employee must be given a reason why this information is being shared.

APPENDIX A

Recommended Document Retention Timescales

The retention period should be the number of years specified plus the current financial period (i.e. three years plus the current period, therefore at least three years documentation will always be retained at any given point in time).

This list is not exhaustive; if you are unsure about any document contact the Parish Clerk or the Senior Assistant for clarification.

Document Retention Period

Finance

Document	**Retention Period**
Financial Published Final Accounts	Indefinitely
Signed Audited Accounts	Indefinitely
Final Account working papers	5 years
Records of all accounting transactions held by the Financial Management System	At least 5 years
Cash Books (records of monies paid out and received)	6 years
Purchase Orders	6 years
Cheque Payment Listings (Invoices received)	6 years
Payment Vouchers Capital and Revenue (copy invoices)	6 years
BACS listings	6 years
Goods received notes, advice notes and delivery notes	3 years
Copy receipts	6 years
Petty cash vouchers and reimbursement claims	6 years
Debtors and rechargeable works records	6 years
Expenses and travel allowance claims	6 years
Asset Register for statutory accounting purposes	10 years
Journal Sheets	5 years
Ledger / Trial Balance	10 years
Year end ledger tabulations – ledger details and cost updates	5 years
Published Budget Books	Indefinitely Medium Term
Financial Plan	Indefinitely
Budget Estimates – Detailed Working Papers and summaries	3 years
Bank Statement (Disk Space) and Instructions to banks	6 years
Bank Statements (Hardcopy)	6 years

Banking Records including Giro cheques, bills of exchange and other negotiable instruments	6 years
Prime evidence that money has been banked	6 years
Refer to Drawer (RD) cheques	2 years
Cancelled Expenditure cheques	2 years
Bank Reconciliation	3 years
Cheques presented / drawn on the Council bank accounts	3 years
Prime records that money has been correctly recorded in the Councils financial systems	3 years
Grant/Funding Applications & Claims	5 years
Precept Forms	Indefinitely
Internal Audit Plans/ Reports	3 years
Fees and Charges Schedules	5 years
Time sheets and overtime claims	6 years
Payroll and tax information relating to employees	6 years
Payroll costing analysis	2 years
Records of payment made to employees for salaries / wages (including intermediate payslips)	6 years
Statutory end of year returns to Inland Revenue and Pensions Section	Indefinitely
Loans and Investment Records; temporary loan receipts and loan tabulations	6 years (after redemption of loan)
VAT, Income Tax and National Insurance Records	6 years
Current and expired insurance contracts and policies indefinitely Insurance records and claims	6 years
Capital and contracts register	Indefinitely
Final accounts of contracts executed under hand	6 years from completion of contract
Final accounts of contracts executed under seal	12 years from completion of contract
All Other reconciliations	3 years

Personnel

Unsuccessful application forms	6 months
Unsuccessful reference requests	1 year

Successful applications forms and CVs	For duration of employment + 5 years
References received	For duration of employment + 5 years
Statutory sick records, pay, calculations, certificates etc.	For duration of employment + 5 years
Annual leave records	For duration of employment + 5 years
Unpaid leave/special leave	For duration of employment + 5 years
Annual appraisal/assessment records	Current year and previous 2 years
Time Control Records	2 years
Criminal Records Bureau Checks	6 months
Personnel files and training records	5 years after employment ceases
Disciplinary or grievance investigations - proved - Verbal –Written –Final warning - Anything involving children	 6 months 1 year 18 months permanently
Disciplinary or grievance investigations - unproven	Destroy immediately after investigation or appeal
Statutory Maternity/Paternity records, calculations, certificates etc	3 years after the tax year in which the maternity period ended
Wages/salary records, overtime, bonuses, expenses etc	6 years

Corporate

Minutes and reports of Committee meetings	Indefinitely
Minutes and reports for Special Committee meetings	Indefinitely
Minutes and reports of sub-committees	Indefinitely
Notes and reports of working groups	Indefinitely
Policies and procedures	Until updated or reviewed
Asset Management records	Indefinitely
Asset management reports	Indefinitely
Internal audit records	3 years
Internal audit fraud investigation	7 years from date of final outcome of investigation
Risk register	Indefinitely
Risk management reports	Indefinitely
Performance reports	Indefinitely

Equalities data	Indefinitely
Questionnaire data	Indefinitely
Details regarding burials	Indefinitely
Drivers log books and mileage	6 years
Vehicle maintenance and registration records (all necessary certificates, MOT certificates , test records and vehicle registration documents etc)	2 years after vehicle disposed of
Fuel usage records	3 years
Allotment application forms	Length of Tenancy + 2 years
Allotment agreements	Length of Tenancy + 2 years
Show health & safety statements	2 Years
Show application including caterers, displays, competition entrants	1 year
Services and equipment quotations – show	1 year
Contacts for show	1 year
Show stalls database inc handcraft and horticulture entrants' details	1 year
trips tenders for coach hire	1 year
Trip database of applicants Coach Tours	1 year
Paper application	1 year
Pre-tender qualification document Summary list of expression of interest received Company contacts A summary of any financial or technical evaluation supplied with the expressions of interest Initial application	1 year
Successful tender documentation Life of contract	6 years
Unsuccessful tender documentation	Until final payment is made
Deeds of land and property	Indefinitely
Land and property rental agreements	6 years after expiry of the agreement
Property evaluation lists	Indefinitely
Lease agreements, variation and valuation queries	6 years after the expiry of the agreement
Documentation referring to externally funded projects	6 years
Booking diaries	3 years
Electronic booking information Is held in the system indefinitely due to the need to gather statistical information	
Premises License applications	Indefinitely

Health & Safety

Health and Safety Accident books	3 years after the date of the last entry (unless an accident involving chemicals or asbestos is contained within
Medical records containing details of employee exposed to asbestos or as specified by the Control of Substances Hazardous to Health Regulations 1999	40 years from the date of the last entry
Medical examination certificates	4 years from date of issue
Records relating to accidents person over 18 years	3 years from date of accident
Records relating to accidents person under 18 years	Until 21st birthday
Asbestos records for premises/property including survey and removal records	40 years
Parks and play area inspection reports	5 years
All inspection certificates (Gas Safe, FENSA etc)	2 years
Repairs job sheets	2 years
Periodic machinery inspection tests (PAT, equipment calibration etc)	2 years
Warranties	10 years
Documents relating to the process of collecting, transporting and disposal of general waste	3 years
Documents relating to the process of collecting, transporting and disposal of hazardous waste	10 years
Plant and equipment testing	2 years
Risk Assessment Forms	2 years
Unusual Incident Forms	3 years
Manual Handling Assessment Forms	3 years

Additional Items	
Approved Minutes	Indefinite
Draft/Rough notes taken at meeting	Until minutes are approved
CCTV	30 days

EAST WITTERING & BRACKLESHAM PARISH COUNCIL DATA PROTECTION TRAINING POLICY

1. East Wittering & Bracklesham Parish Council ensures that those with day-to-day responsibility for enabling the demonstration of compliance with the General Data Protection Regulation (GDPR) and good practice are able to demonstrate competence in their understanding of the GDPR and good practice, and how this should be implemented within East Wittering & Bracklesham Parish Council.
2. The Clerk keeps records of the relevant training undertaken by each person who has this level of responsibility.
3. East Wittering & Bracklesham Parish Council also ensures that these staff members remain informed about issues related to the management of personal information, where appropriate, by contact with external bodies. East Wittering & Bracklesham Parish Council maintains a list of relevant external bodies, the most important of which is the Information Commissioner's Office (www.ico.gov.uk)
4. East Wittering & Bracklesham Parish Council ensures that all staff understand their responsibility to ensure that personal information is protected and processed in accordance with East Wittering & Bracklesham Parish Council's procedures, taking into account any related security requirements.
5. All employees/staff are given training to enable them to process personal information in accordance with East Wittering & Bracklesham Parish Council's procedures. This training is relevant to the role that each employee performs within East Wittering & Bracklesham Parish Council
6. The Clerk is responsible for organising relevant training for responsible individuals and staff generally, and for maintaining records of the attendance of staff at relevant training at appropriate times across East Wittering & Bracklesham Parish Council's business cycle.

EAST WITTERING & BRACKLESHAM PARISH COUNCIL - 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 East Wittering & Bracklesham Parish Council which is the data controller for your data.

Other data controllers the council works with:

- Local authorities
- Community groups
- Charities
- Other not for profit entities
- Contractors
- Credit reference agencies

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 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 dependants;

- Where you pay for activities such as use of a council hall or room, financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers;
- The personal data we process may include sensitive or other special categories of personal data such as criminal convictions, racial or ethnic origin, mental and physical health, details of injuries, medication/treatment received, political beliefs, trade union affiliation, genetic data, biometric data, data concerning and sexual life or orientation.
- 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 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.
- 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 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 hall rental 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 7 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 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.

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.

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.

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).

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.

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.

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 visiting this website https://gdpr-info.com/data-protection-contact-form/ or email.

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/contactus/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.

CHANGES TO THIS NOTICE

We keep this Privacy Notice under regular review and we will place any updates on this web page www.ewbpc.org.uk. This Notice was last updated in May 2018.

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 East Wittering & Bracklesham Parish Council Data Protection Officer: GDPR-Info Ltd Email: dpo@gdpr-info.com

EAST WITTERING & BRACKLESHAM PARISH COUNCIL SUBJECT ACCESS REQUEST POLICY

1. Scope

All personal data processed by East Wittering & Bracklesham Parish Council is within the scope of this procedure. This procedure excludes personal data that is asked for as a matter of routine by data subjects

Data subjects are entitled to ask

· Whether East Wittering & Bracklesham Parish Council is processing any personal data about that individual and, if so, to be given:

- a description of the personal data;
- the purposes for which it is being processed; and,
- details of who will be allowed to see the personal data.

· To be given a copy of the information and to be told about the sources from which East Wittering & Bracklesham Parish Council derived the information; and

· Where appropriate, logic involved in any automated decisions relating to them.

2. Responsibilities

GDPR-*info* Ltd are responsible for the application and effective working of this procedure, and for reporting to the Parish Clerk on Subject Access Requests (SARs).

GDPR-*info* Ltd is responsible for handling all SARs.

3. Procedure

3.1 Subject Access Requests must be made using our web page https://gdpr-info.com/dataprotection-contact-form/

3.2 The data subject must provide evidence as to identity.

3.3 The data subject must identify the data that is being requested and where it is being held and this information must be shown on the SAR application form. Note that the data subject is entitled to ask for all data that East Wittering & Bracklesham Parish Council holds, without specifying that data.

3.4 The date by which the identification checks, and the specification of the data sought must be recorded; East Wittering & Bracklesham Parish Council has one month from this date to provide the requested information. There are no circumstances in which an extension to that one month will be provided, and failure to provide the requested information within that one month is a breach of the GDPR.

3.5 The SAR application is immediately forwarded to GDPR-info Ltd, who will ensure that the requested data is collected within the time frame.

Collection will entail either:

3.5.1 Collecting the data specified by the data subject, or

3.5.2 Searching all databases and all relevant filing systems (manual files) in East Wittering & Bracklesham Parish Council, including all back up and archived files, whether computerised or manual, and including all e-mail folders and

archives. The Parish Clerk maintains a data map that identifies where all data in East Wittering & Bracklesham Parish Council is stored.

3.6 GDPR-info Ltd maintains a record of requests for data and of its receipt, including dates. Note that data may not be altered or destroyed in order to avoid disclosing it.

3.7 GDPR-info Ltd is responsible for reviewing all provided documents to identify whether any third parties are identified in it and for either excising identifying third party information from the documentation or obtaining written consent from the third party for their identity to be revealed.

3.8 If the requested data falls under one of the following exemptions, it does not have to be provided:

3.8.1 Crime prevention and detection.

3.8.2 Negotiations with the requester.

3.8.3 Management forecasts.

3.8.4 Confidential references given by East Wittering & Bracklesham Parish Council (not ones given to East Wittering & Bracklesham Parish Council).

3.8.5 Information used for research, historical or statistical purposes.

3.8.6 Information covered by legal professional privilege.

3.9 The information is provided to the data subject in electronic format unless otherwise requested and all the items provided are listed on a schedule that shows the data subject's name and the date on which the information is delivered.

3.10 The electronic formats used for responses to SARs are:

3.10.1 .CSV file

Date GDPR Policies adopted: 11/05/23

Minute ref: 23.66.5