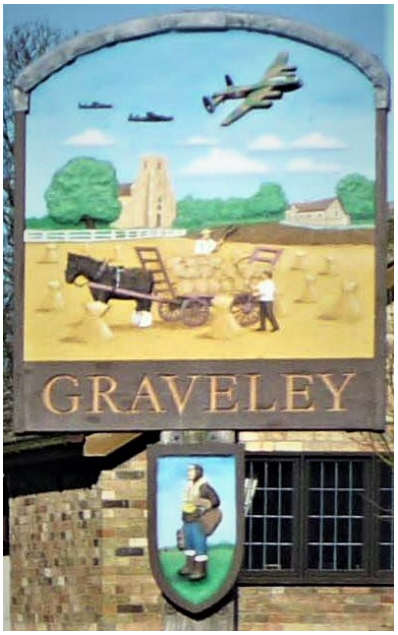

Information and Data Protection Policy

Document Configuration Management & Control

Version	Description	Originated	Approved	Minute Ref.
Version 1	Annual Review	04/01/2023	23/05/2023	23/24-37.3

Table of Contents

Introduction

In order to conduct its business, services and duties, Graveley Parish Council processes a wide range of data, relating to its own operations and some which it handles on behalf of partners. In broad terms, this data can be classified as:

- Data shared in the public arena about the services it offers, its mode of operations and other information it is required to make available to the public.
- Confidential information and data not yet in the public arena such as ideas or policies that are being worked up.
- Confidential information about other organisations because of commercial sensitivity.
- Personal data concerning its current, past and potential employees, Councillors, and volunteers.
- Personal data concerning individuals who contact it for information, to access its services or facilities or to make a complaint.

Graveley Parish Council will adopt procedures and manage responsibly, all data which it handles and will respect the confidentiality of both its own data and that belonging to partner organisations it works with and members of the public. In some cases, it will have contractual obligations towards confidential data, but in addition will have specific legal responsibilities for personal and sensitive information under data protection legislation.

The Parish Council will periodically review and revise this policy in the light of experience, comments from data subjects and guidance from the Information Commissioners Office.

The Council will be as transparent as possible about its operations and will work closely with public, community and voluntary organisations. Therefore, in the case of all information which is not personal or confidential, it will be prepared to make it available to partners and members of Graveley's communities. Details of information which is routinely available is contained in the Council's Publication Scheme which is based on the statutory model publication scheme for local councils.

Protecting Confidential or Sensitive Information

Graveley Parish Council recognises it must at times, keep and process sensitive and personal information about both employees and the public, it has therefore adopted this policy not only to meet its legal obligations but to ensure high standards.

The General Data Protection Regulations (GDPR) which become law on 25th May 2018 and will, like the Data Protection Act 1998 before them, seek to strike a balance between the rights of individuals and the sometimes, competing interests of those such as the Parish Council with legitimate reasons for using personal information.

The policy is based on the premise that Personal Data must be:

- Processed fairly, lawfully and in a transparent manner in relation to the data subject.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date.
- Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- 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.

Data Protection Terminology

Data subject - means the person whose personal data is being processed.
That may be an employee, prospective employee, associate or prospective associate of GPC or someone transacting with it in some way, or an employee, Member or volunteer with one of our clients, or persons transacting or contracting with one of our clients when we process data for them.

Personal data - means any information relating to a natural person or data subject that can be used directly or indirectly to identify the person.
It can be anything from a name, a photo, and an address, date of birth, an email address, bank details, and posts on social networking sites or a computer IP address.

Sensitive personal data - includes information about racial or ethnic origin, political opinions, and religious or other beliefs, trade union membership, medical information, sexual orientation, genetic and biometric data or information related to offences or alleged offences where it is used to uniquely identify an individual.

Data controller - means a person who (either alone or jointly or in common with other persons) (e.g., Parish Council, employer, council) determines the purposes for which and the manner in which any personal data is to be processed. In this case, Graveley Parish Council is the data controller.

Data processor - in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Processing information or data - means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- organising, adapting or altering it

- retrieving, consulting or using the information or data
- disclosing the information or data by transmission, dissemination or otherwise making it available
- aligning, combining, blocking, erasing or destroying the information or data. regardless of the Technology used.

Graveley Parish Council processes **personal data** in order to:

- fulfil its duties as an employer by complying with the terms of contracts of employment, safeguarding the employee and maintaining information required by law.
- pursue the legitimate interests of its business and its duties as a public body, by fulfilling contractual terms with other organisations, and maintaining information required by law.
- monitor its activities including the equality and diversity of its activities
- fulfil its duties in operating the business premises including security
- assist regulatory and law enforcement agencies
- process information including the recording and updating details about its Councillors, employees, partners and volunteers.
- process information including the recording and updating details about individuals who contact it for information, or to access a service, or make a complaint.
- undertake surveys, censuses and questionnaires to fulfil the objectives and purposes of the Council.
- undertake research, audit and quality improvement work to fulfil its objects and purposes.
- carry out Council administration.

Where appropriate and governed by necessary safeguards we will carry out the above processing jointly with other appropriate bodies from time to time.

The Council will ensure that at least one of the following conditions is met for personal information to be considered fairly processed:

- The individual has consented to the processing
- Processing is necessary for the performance of a contract or agreement with the individual
- Processing is required under a legal obligation
- Processing is necessary to protect the vital interests of the individual
- Processing is necessary to carry out public functions
- Processing is necessary in order to pursue the legitimate interests of the data controller or third parties.

Particular attention is paid to the processing of any **sensitive personal information** and the Parish Council will ensure that at least one of the following conditions is met:

- Explicit consent of the individual
- Required by law to process the data for employment purposes
- A requirement in order to protect the vital interests of the individual or another person

Who is responsible for protecting a person's personal data?

The Parish Council as a corporate body has ultimate responsibility for ensuring compliance with the Data Protection legislation. The Council has delegated this responsibility day to day to the Clerk.

- Email: clerk@graveleycambspc.org.uk
- Phone: 01480 830605
- Correspondence: The Clerk, 10 Church End, Hilton, PE28 9NJ

Diversity Monitoring

Graveley Parish Council may monitor the diversity of its employees, and Councillors, in order to ensure that there is no inappropriate or unlawful discrimination in the way it conducts its activities. It may undertake similar data handling in respect of prospective employees. This data will always be treated as confidential. It will only be accessed by authorised individuals within the Council and will not be disclosed to any other bodies or individuals. Diversity information will never be used as selection criteria and will not be made available to others involved in the recruitment process. Anonymised data derived from diversity monitoring may be used for monitoring purposes and may be published and passed to other bodies.

The Council will always give guidance on personnel data to employees, councillors, partners and volunteers through a Privacy Notice and ensure that individuals on whom personal information is kept are aware of their rights and have easy access to that information on request.

Appropriate technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
Personal data shall not be transferred to a country or territory outside the European Economic Areas unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Information provided to us

The information provided (personal information such as name, address, email address, phone number) will be processed and stored so that it is possible for us to contact, respond to or conduct the transaction requested by the individual. By transacting with Graveley Parish Council, individuals are deemed to be giving consent for their personal data provided to be used and transferred in accordance with this policy, however

wherever possible specific written consent will be sought. It is the responsibility of those individuals to ensure that the Parish Council is able to keep their personal data accurate and up-to-date. The personal information will be not shared or provided to any other third party or be used for any purpose other than that for which it was provided.

The Councils Right to Process Information

General Data Protection Regulations (and Data Protection Act) Article 6 (1) (a) (b) and (e), summarised below:
Processing is with consent of the data subject, or
Processing is necessary for compliance with a legal obligation.
Processing is necessary for the legitimate interests of the Council.

Article 6 (1):
(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
(b) 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) processing is necessary for compliance with a legal obligation to which the controller is subject;
(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
(e) 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;
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. [But this point shall not apply to processing carried out by public authorities in the performance of their tasks.]

If relying on consent as the ground for processing personal data, note that 'opt-out' types of response are insufficient. Article 4(11) of the GDPR says that consent means: 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'.

Note that the processing of special categories of personal data is prohibited unless one or more of the conditions in Article 9 of the GDPR applies. The functional work of a local authority and the holding of relevant data about an employee of the council are both good reasons to hold and process it. The best way to hold 'special categories of personal data' however is to do it with the explicit written consent of the data subject

Information Security

The Parish Council cares 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 appropriate policies.
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.

Children

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

Rights of a Data Subject

Individuals have various rights in respect of their own personal data. This requires the controller to provide data subjects with information at the time information is collected from them (e.g., through privacy notices) (Article 13) and to respond to individual data subject requests (Article 15) and the exercise of other rights.

The controller must provide the information or communications in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The controller must respond to a subject access request (and to some other specified types of requests) within one month of receipt of the request, but this period may be extended by a further two months where necessary, considering the complexity and number of requests. The information should be provided free of charge. But if the requests are manifestly unfounded or excessive, in particular because of their repetitive character, the controller has the option of either charging a reasonable fee or refusing to act on the request. (Article 12).

Information about other data subject rights can be found in the relevant Articles of the GDPR, including:

- rectification (Article 16)
- erasure (or the right 'to be forgotten') (Article 17)
- restriction of processing (Article 18)
- data portability (Article 20)
- to object (Article 21)
- not to be subject to a decision based solely on automated processing (Article 22).

These data subject rights are rights given to individuals in connection with information processed by a controller about the data subject. An individual has no right under GDPR to access information about anyone else.

Access to Information: an individual has the right to request access to the information we have on them. They can do this by contacting our Clerk – please see Subject Access Request form in Appendix 3.

Information Correction: If they believe that the information we have about them is incorrect, they may contact us so that we can update it and keep their data accurate. Please contact: Clerk.

Information Deletion: If the individual wishes the Parish Council to delete the information about them, they can do so by contacting the Clerk.

Right to Object: If an individual believes their data is not being processed for the purpose it has been collected for, they may object by contacting the Clerk.

The Parish Council does not use automated decision making or profiling of individual personal data.

Complaints: If an individual has a complaint regarding the way their personal data has been processed, they may make a complaint to the Clerk or the Information Commissioners Office casework@ico.org.uk Tel: 0303 123 1113.

The Council will ensure that individuals on whom personal information is kept are aware of their rights and have easy access to that information on request.

Making Information Available

The Publication Scheme is a means by which the Council can make a significant amount of information available routinely, without waiting for someone to specifically request it. The scheme is intended to encourage local people to take an interest in the work of the Council and its role within the community.

In accordance with the provisions of the Freedom of Information Act 2000, this Scheme specifies the classes of information which the Council publishes or intends to publish.

All formal meetings of Council and its committees are subject to statutory notice being given on notice boards and the Website. The Council publishes an annual programme in May each year. All formal meetings are open to the public and press and reports to those meetings and relevant background papers are available for the public to see. The Council welcomes public participation and has a public participation session on each Council and committee meeting. Details can be seen in the Council's Standing Orders, which are available on its Website.

Occasionally, Council or committees may need to consider matters in private. Examples of this are matters involving personal details of staff, or a particular member of the public, or where details of commercial/contractual sensitivity are to be discussed. This will only

happen after a formal resolution has been passed to exclude the press and public and reasons for the decision are stated. Minutes from all formal meetings, including the confidential parts are public documents.

The Openness of Local Government Bodies Regulations 2014 requires written records to be made of certain decisions taken by officers under delegated powers. These are not routine operational and administrative decisions such as giving instructions to the workforce or paying an invoice approved by Council but would include urgent action taken after consultation with the Chairman, such as responding to a planning application in advance of Council. In other words, decisions which would have been made by Council or committee had the delegation not been in place.

The 2014 Regulations also amend the Public Bodies (Admission to Meetings) Act 1960 to allow the public or press to film, photograph or make an audio recording of council and committee meetings normally open to the public. The Council will where possible facilitate such recording unless it is being disruptive. It will also take steps to ensure that children, the vulnerable and members of the public who object to being filmed are protected without undermining the broader purpose of the meeting.

The Council will be pleased to make special arrangements on request for persons who do not have English as their first language or those with hearing or sight difficulties.

Fees

Under the (outgoing) Data Protection Act 1998, a Data Controller had to "notify" the Information Commissioner's Office (ICO). This was in effect a registration procedure and it came at a cost (£35 a year for most local councils; or £500 a year for local councils with more than 250 employees). From 1 April 2018 new arrangements will apply under Regulations to be made under section 108 of the Digital Economy Act 2017. The Information Commissioner has indicated that councils will not need to "notify" the ICO in the same way, but will need to pay a data protection fee, unless an exemption applies. Further information will be available on the ICO website. Graveley Parish Council pays an annual data protection fee to the ICO.

Appendix 1 – Privacy Notice

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 Regulations Article 6 (1) (a) (b) and (e)

Processing is with consent of the data subject or
Processing is necessary for compliance with a legal obligation or
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

Graveley Parish 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 appropriate policies. Copies of these policies can be requested.

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 Graveley Parish 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 our Clerk.

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 Clerk to request this.

Information Deletion

If you wish Graveley Parish Council to delete the information about you please contact the 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 Clerk to object.

Rights Related to Automated Decision Making and Profiling

Graveley Parish 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 constantly review our Privacy Policies to keep it up to date in protecting your data. (You can request a copy of our policies at any time).

Complaints

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

Appendix 2 – Privacy Impact Assessment

As part of the PIA process organisations should describe how information is collected, stored, used and deleted.

Project Name	

What is the Projects Outcome	
Information to be obtained	
What is the information to be used for?	
Who will obtain it?	
Who will have access to the information?	
Any other Information?	
Identify Possible Privacy Risks Risks to individuals, Corporate Risks, Compliance Risks, Associated Organisation/Corporate Risk	
Identify how to mitigate these Risks Risk, Solution, Result and Evaluation.	
Evaluate costs involved	
Recourses required for the project	

Review Process Who will action the review? When will it be reviewed? Action to be take Date for completion Responsibility for action. Lessons learnt	

What to think about when preparing the Privacy Impact Assessment.

This form is to be used in conjunction with Conducting Privacy Impact Assessments Code of Practice.

It can be integrated with consultation or planning processes. Effective consultation internally within the Council is an important part of any Privacy Impact Assessment (PIA). Data protection risks are more likely to remain unmitigated on projects which have not involved discussions with the people building a system or carrying out procedures.

Screening questions to help you decide whether a Privacy Impact Assessment is required:

Will the project involve the collection of new information about individuals?

Will the project compel individuals to provide information about themselves?

Will information about individuals be disclosed to Organisations or people who have not previously had routine access to the information?

Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?

Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.

Will the project result in you making decisions or acting against individuals in ways which can have a significant impact on them?

Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.

Will the project require you to contact individuals in ways which they may find intrusive?

When preparing your Privacy Impact Assessment you need to identify the below possible Stake holders.

- Project management team
  The team responsible for the overall implementation of a project will play a central role in the PIA process.

- Data protection officer
  If an organisation has a dedicated DPO, they are likely to have a close link to a PIA. Even if project managers are responsible for individual PIAs, the DPO will be able to provide specialist knowledge on privacy issues,

- Engineers, developers and designers
  The people who will be building a product need to have a clear understanding of how to approach privacy issues. They will also be able to suggest workable privacy solutions to the risks which have been identified.

- Information technology (IT)

  Will be able to advise on security risks and solutions. The role of IT is limited to security, and might also include discussions on the usability of any software.

- Procurement
  If the project will require systems or services to be procured, the needs of the project need to be established before procurement takes place.

- Potential suppliers and data processors
  If some of the project will be outsourced to a third party, early engagement will help to understand which options are available.

- Communications
  A PIA can become a useful part of a project's communication strategy. For example, involving communications colleagues in the PIA can help to establish a clear message to the public about a project.

- Customer-facing roles
  It is important to consult with the people who will have to use a new system or put a policy into practice. They will be able to advise on whether the system will work as intended.

- Corporate governance/compliance
  Colleagues who work on risk management for an organisation should be able to integrate PIAs into their work. Other areas of compliance can be included in the PIA process.

- Researchers, analysts, and statisticians
  Information gathered by a new project may be used to analysing customer behaviour or for other statistical purposes. Where relevant, consulting with researchers can lead to more effective safeguards such as anonymisation.

- Senior management
  It will be important to involve those with responsibility for signing off or approving a project.

External Consultation

External consultation means seeking the views of the people who will be affected by the project. This may be members of the public but can also mean people within an organisation (for example staff who will be affected by a new online HR system). Consultation with the people who will be affected is an important part of the PIA process. There are two main aims. Firstly, it enables an organisation to understand the concerns of those individuals. The consultation will also improve transparency by making people aware of how information about them is being used.

A thorough assessment of privacy risks is only possible if an organisation fully understands how information is being used in a project. An incomplete understanding of how information is used can be a significant privacy risk – for example; data might be used for unfair purposes or disclosed inappropriately.

You must have regard when linking to the Privacy Impact Assessment to the 8 Data Protection principals below:

Principle 1

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

a) at least one of the conditions in Schedule 2 is met, and

b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

Have you identified the purpose of the project?
How will individuals be told about the use of their personal data?
Do you need to amend your privacy notices?
Have you established which conditions for processing apply?
If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?
If your organisation is subject to the Human Rights Act, you also need to consider:
Will your actions interfere with the right to privacy under Article 8?
Have you identified the social need and aims of the project?
Are your actions a proportionate response to the social need?

Principle 2

Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.

Does your project plan cover all of the purposes for processing personal data?
Have potential new purposes been identified as the scope of the project expands?

Principle 3
Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
Is the information you are using of good enough quality for the purposes it is used for?
Which personal data could you not use, without compromising the needs of the project?

Principle 4
Personal data shall be accurate and, where necessary, kept up to date.
If you are procuring new software does it allow you to amend data when necessary?
How are you ensuring that personal data obtained from individuals or other organisations is accurate?

Principle 5
Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.
What retention periods are suitable for the personal data you will be processing?
Are you procuring software which will allow you to delete information in line with your retention periods?

Principle 6
Personal data shall be processed in accordance with the rights of data subjects under this Act.
Will the systems you are putting in place allow you to respond to subject access requests more easily?
If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?

Principle 7
Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
Do any new systems provide protection against the security risks you have identified?
What training and instructions are necessary to ensure that staff know how to operate a new system securely?

Principle 8
Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.
Will the project require you to transfer data outside of the EEA?
If you will be making transfers, how will you ensure that the data is adequately protected?

Appendix 3 – Subject Access Request Form

Process to Action		
Name of requester (Method of communication) Email Address Phone number Postal Address		
Date Subject Access Request made		
Is the request made under the Data Protection Legislation	Yes	No
Date Subject Access Request action to be completed by (One month after receipt time limit)		
Extension to the date of reply requested (An extension of another two months is permissible provided it is communicated to the subject within the one-month period)	Yes	No
Extension date advised to the Subject Requester and method of contact		
Identification must be proven from the below list: Current UK/EEA Passport UK Photo card Driving Licence (Full or Provisional) EEA National Identity Card Full UK Paper Driving Licence State Benefits Entitlement Document State Pension Entitlement Document HMRC Tax Credit Document Local Authority Benefit Document State/Local Authority Educational Grant Document HMRC Tax Notification Document Disabled Driver's Pass Financial Statement issued by bank, building society or credit card company Utility bill for supply of gas, electric, water or telephone landline A recent Mortgage Statement A recent council Tax Bill/Demand or Statement Tenancy Agreement Building Society Passbook which shows a transaction in the last 3 months and their address		
Verification sought that the Subject Access request is substantiated	Yes	No
Verification received	Yes	No
Verification if the Council cannot provide the information requested	Yes	No
Is the request excessive or unfounded?	Yes	No
Request to be actioned	Yes	No

Fee to be charged (Subject Access requests must be undertaken free of charge to a requester unless the legislation permits a reasonable charge)	Yes	No
If the request is to be refused, action to be taken and by whom.		
Changes requested to data/ or removal		
Complaint Process (Where a requestor is not satisfied with a response to a SAR, the council must manage this as a complaint)		
Completion date of request		
Date complaint received by requested and details of the complaint		
Date complaint completed and outcome		

Categories of Data to Check

Data	Filing Cabinet	Laptop	Checked	Corrected/ Deleted	Actioned by
HR					
Democracy					
Statutory Function					
Legal					
Business					
Legal requirement					
General Data					
Consultation Data					

Appendix 4 – Data Security Breach Reporting Form

A “personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed (Article 4(12)).

A data security breach can happen for a number of reasons: Loss or theft of data or equipment on which data is stored, inappropriate access controls allowing unauthorised use, equipment failure, human error, unforeseen circumstances such as a fire or flood, hacking attack, ‘blagging’ offences where information is obtained by deceiving the organisation who holds it. Use this form to report such breaches.
Example: reportable theft or loss of an unencrypted laptop computer or other unencrypted portable electronic/digital media holding names, addresses, dates of birth and National Insurance numbers of individuals. A manual paper-based filing system (or unencrypted digital media) holding the personal data relating to named individuals and their financial records etc. More information can be found using the below link:
https://ico.org.uk/media/for-organisations/documents/1562/guidance_on_data_security_breach_management.pdf

Breach Containment and Recovery

Article 2(2) of the Notification Regulation states:
The provider shall notify the personal data breach to the competent national authority no later than 24 hours after the detection of the personal data breach, where feasible. The provider shall include in its notification to the competent national authority the information set out in Annex I. The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) provide rules about sending marketing and advertising by electronic means, such as by telephone, fax, email, text and picture or video message, or by using an automated calling system. PECR also include other rules relating to cookies, telephone directories, traffic data, location data and security breaches. Detection of a personal data breach shall be deemed to have taken place when the provider has acquired sufficient awareness that a security incident has occurred that led to personal data being compromised, in order to make a meaningful notification as required under this Regulation.

When a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller must communicate the personal data breach to the data subject without undue delay, unless specific conditions apply. These conditions include the implementation of technical measures such as encryption which would render the data unintelligible to any person not authorised to access it, or the taking of measures to contain the initial high risk, or it would involve disproportionate effort (in which case a public communication or similar measure can be used to inform data subjects) (Article 34).

Date and time of Notification of Breach	
Notification of Breach to whom Name Contact Details	
Details of Breach	
Nature and content of Data Involved	
Number of individuals affected:	
Name of person investigating breach Name Job Title Contact details Email Phone number Address	
Information Commissioner informed Time and method of contact https://report.ico.org.uk/security-breach/	

Police Informed if relevant Time and method of contact Name of person contacted Contact details	
Individuals contacted How many individuals contacted? Method of contact used to contact. Does the breach affect individuals in other EU member states? What are the potential consequences and adverse effects on those individuals? Confirm that details of the nature of the risk to the individuals affected: any measures they can take to safeguard against it; and the likely cost to them of taking those measures is relayed to the individuals involved.	
Staff briefed	
Assessment of ongoing risk	
Containment Actions: technical and organisational security measures have you applied (or were to be applied) to the affected personal data	

Recovery Plan	
Evaluation and response	

Appendix 5 – GDPR Awareness Checklist for Councillors

Whilst Parish Councils are expected to comply with GDPR, individual councillors will also need to ensure that they protect an individual's personal data whether it is stored electronically or as a hard copy. This applies only to living individuals (not the deceased, companies, other authorities and charities)

Personal data includes:

- Names and addresses
- Telephone numbers
- Email addresses
- IP addresses

The following measures are recommended to help councillors comply with GDPR:

Action	**Noted** ü
Set up a separate email account for parish council correspondence	
Ensure that all devices (computers, laptops, phones) are password protected	
Do not forward on emails or email threads as they may contain personal data	
Copy and paste information from an email if you want to pass it on, rather than forwarding on an email to remove the IP address from the header.	
Where possible direct all correspondence to the clerk who can obtain the necessary consent	
Where possible avoid holding an individual's information in a councillor's home or on a councillor's own PC. If a councillor has to hold any information containing personal data on behalf of the Parish Council, it needs to be stored securely in a locked room or cabinet or if on a PC, in an encrypted folder.	
Make sure your antivirus software and operating system are up-to-date	
Make sure your computer's firewall is turned on	
Inform the Clerk of any breaches within 48 hours	

I confirm that I have read the information above and understand my responsibility as a parish councillor for protecting personal data.

Signed: Date: