Dittisham Parish Council
Information & Data Protection Policy

Introduction

In order to conduct its business, services and duties, Dittisham 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.

Dittisham 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 the Parish'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

Dittisham 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 Regulation (GDPR) which became law on 25th May 2018 and like the Data Protection Act 1998 before, seeks to strike a balance between the rights of individuals and the sometimes, competing interests of those such as Parish and Town Councils 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 Dittisham Parish Council 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.

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.

Dittisham 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

Data Protection Impact Assessment (DPIA)
Following guidance available from the ICO, the Parish Council must do a DPIA for processing that is **likely to result in a high risk** to individuals; This includes both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm. This includes some specified types of processing. The ICO provide screening checklist to help the Parish Council decide when to do a DPIA, and a model assessment form is available. These are provided as an appendix to this policy.

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 Parish Clerk.

- Email: parishclerk@dittishamparish.co.uk
- Phone: 07979 381356
- Correspondence: The Parish Clerk, c/o The Bungalow, Old Road, Harbertonford, Totnes, TQ9 7TA

Diversity Monitoring
Dittisham 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 undertakes 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 will 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 Dittisham 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 where ever 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)
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.

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

Access to Information: an individual has the right to request access to the information we have on them. They can do this by contacting the Parish Clerk or Data Protection Officer, should one be appointed.

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 the Parish Clerk.

Information Deletion: If the individual wishes the Parish Council to delete the information about them, they can do so by contacting the Parish 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 Parish Clerk or Data Protection Officer should one have been appointed.

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 Parish Clerk, Data Protection Officer 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. It is supplemented with an Information Guide which will give greater detail of what the Council will make available and hopefully make it easier for people to access it.

All formal meetings of Council and its committees are subject to statutory notice being given on notice boards and the Parish Council's website. 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 the Parish Council 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.

Disclosure Information
The Council will as necessary undertake checks on both staff and Members with the Disclosure and Barring Service and will comply with their Code of Conduct relating to the secure storage, handling, use, retention and disposal of Disclosures and Disclosure Information. It will include an appropriate operating procedure in its integrated quality management system.

Data Transparency
The Council has resolved to act in accordance with the Code of Recommended Practice for Local Authorities on Data Transparency (September 2011). This sets out the key principles for local authorities in creating greater transparency through the publication of public data and is intended to help them meet obligations of the legislative framework concerning information.

"Public data" means the objective, factual data on which policy decisions are based and on which public services are assessed, or which is collected or generated in the course of public service delivery.

The Code will therefore underpin the Council's decisions on the release of public data and ensure it is proactive in pursuing higher standards and responding to best practice as it develops.

The principles of the Code are:
Demand led: new technologies and publication of data should support transparency and accountability
Open: the provision of public data will be integral to the Council's engagement with residents so that it drives accountability to them.
Timely: data will be published as soon as possible following production.

Government has also issued a further Code of Recommended Practice on Transparency, compliance of which is compulsory for parish councils with turnover (gross income or gross expenditure) not exceeding £25,000 per annum. These councils will be exempt from the requirement to have an external audit from April 2017. Dittisham Parish Council exceeds this turnover but will never the less ensure the following information is published on its website for ease of access:

- All transactions above £100.
- End of year accounts
- Annual Governance Statements
- Internal Audit Reports
- List of Councillor or Member responsibilities
- Details of public land and building assets
- Draft minutes of Council and committees within one month
- Agendas and associated papers no later than three clear days before the meeting.

APPENDIX

Data Protection Impact Assessment

Guidance from ICO website: 1st April 2026

What is a DPIA?
A DPIA is a way for you to systematically and comprehensively analyse your processing and help you identify and minimise data protection risks.

DPIAs should consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm – to individuals or to society at large, whether it is physical, material or non-material.

To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals.
A DPIA does not have to indicate that all risks have been eradicated. But it should help you document them and assess whether or not any remaining risks are justified.

DPIAs are a legal requirement for processing that is likely to be high risk. But an effective DPIA can also bring broader compliance, financial and reputational benefits, helping you demonstrate accountability and building trust and engagement with individuals.

A DPIA may cover a single processing operation or a group of similar processing operations. A group of controllers can do a joint DPIA.

It's important to embed DPIAs into your organisational processes and ensure the outcome can influence your plans. A DPIA is not a one-off exercise. You should see it as an ongoing process that is subject to regular review.

When do we need a DPIA?

You must do a DPIA before you begin any type of processing that is "likely to result in a high risk". This means that although you have not yet assessed the actual level of risk, you need to screen for factors that point to the potential for a widespread or serious impact on individuals.

In particular, the UK GDPR says you must do a DPIA if you plan to:

- use systematic and extensive profiling with significant effects;
- process special category or criminal offence data on a large scale; or
- systematically monitor publicly accessible places on a large scale.
-

When considering if your processing is likely to result in high risk, you should consider the relevant European guidelines. These define nine criteria of processing operations likely to result in high risk. While the guidelines suggest that, in most cases, any processing operation involving two or more of these criteria requires a DPIA, you may consider in your case that just meeting one criterion could require a DPIA.

The ICO also requires you to do a DPIA if you plan to:

- use innovative technology (in combination with any of the criteria from the European guidelines);
- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;
- process biometric data (in combination with any of the criteria from the European guidelines);
- process genetic data (in combination with any of the criteria from the European guidelines);
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing') (in combination with any of the criteria from the European guidelines);
- track individuals' location or behaviour (in combination with any of the criteria from the European guidelines);
- profile children or target marketing or online services at them; or
- process data that might endanger the individual's physical health or safety in the event of a security breach.

You should also think carefully about doing a DPIA for any other processing that is large scale, involves profiling or monitoring, decides on access to services or opportunities, or involves sensitive data or vulnerable individuals.
Even if there is no specific indication of likely high risk, it is good practice to do a DPIA for any major new project involving the use of personal data. You can use or adapt the checklists to help you carry out this screening exercise.

Checklists

DPIA awareness checklist

☐ We provide training so that our staff understand the need to consider a DPIA at the early stages of any plan involving personal data.
☐ Our existing policies, processes and procedures include references to DPIA requirements.
☐ We understand the types of processing that require a DPIA, and use the screening checklist to identify the need for a DPIA, where necessary.
☐ We have created and documented a DPIA process.
☐ We provide training for relevant staff on how to carry out a DPIA.

DPIA screening checklist

☐ We consider carrying out a DPIA in any major project involving the use of personal data.
☐ We consider whether to do a DPIA if we plan to carry out any other:
☐ evaluation or scoring;
☐ automated decision-making with significant effects;
☐ systematic monitoring;
☐ processing of sensitive data or data of a highly personal nature;
☐ processing on a large scale;
☐ processing of data concerning vulnerable data subjects;
☐ innovative technological or organisational solutions;
☐ processing that involves preventing data subjects from exercising a right or using a service or contract.
☐ We always carry out a DPIA if we plan to:
☐ use systematic and extensive profiling or automated decision-making to make significant decisions about people;
☐ process special-category data or criminal-offence data on a large scale;
☐ systematically monitor a publicly accessible place on a large scale;
☐ use innovative technology in combination with any of the criteria in the European guidelines;
☐ use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit;
☐ carry out profiling on a large scale;
☐ process biometric or genetic data in combination with any of the criteria in the European guidelines;
☐ combine, compare or match data from multiple sources;
☐ process personal data without providing a privacy notice directly to the individual in combination with any of the criteria in the European guidelines;
☐ process personal data in a way that involves tracking individuals' online or offline location or behaviour, in combination with any of the criteria in the European guidelines;
☐ process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them;
☐ process personal data that could result in a risk of physical harm in the event of a security breach.
☐ We carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing.
☐ If we decide not to carry out a DPIA, we document our reasons.

DPIA process checklist

☐ We describe the nature, scope, context and purposes of the processing.
☐ We ask our data processors to help us understand and document their processing activities and identify any associated risks.
☐ We consider how best to consult individuals (or their representatives) and other relevant stakeholders.

☐ We ask for the advice of our data protection officer.
☐ We check that the processing is necessary for and proportionate to our purposes, and describe how we will ensure compliance with data protection principles.
☐ We do an objective assessment of the likelihood and severity of any risks to individuals' rights and interests.
☐ We identify measures we can put in place to eliminate or reduce high risks.
☐ We record our decision-making in the outcome of the DPIA, including any difference of opinion with our DPO or individuals consulted.
☐ We implement the measures we identified, and integrate them into our project plan.
☐ We consult the ICO before processing, if we cannot mitigate high risks.
☐ We keep our DPIAs under review and revisit them when necessary.

Have we written a good DPIA?
A good DPIA helps you to evidence that:

- you have considered the risks related to your intended processing; and
- you have met your broader data protection obligations.

This checklist will help ensure you have written a good DPIA.

☐ confirmed whether the DPIA is a review of pre-GDPR processing or covers intended processing, including timelines in either case;
☐ explained why we needed a DPIA, detailing the types of intended processing that made it a requirement;
☐ structured the document clearly, systematically and logically;
☐ written the DPIA in plain English, with a non-specialist audience in mind, explaining any technical terms and acronyms we have used;
☐ set out clearly the relationships between controllers, processors, data subjects and systems, using both text and data-flow diagrams where appropriate;
☐ ensured that the specifics of any flows of personal data between people, systems, organisations and countries have been clearly explained and presented;
☐ explicitly stated how we are complying with each of the Data Protection Principles under GDPR and clearly explained our lawful basis for processing (and special category conditions if relevant);
☐ explained how we plan to support the relevant information rights of our data subjects;
☐ identified all relevant risks to individuals' rights and freedoms, assessed their likelihood and severity, and detailed all relevant mitigations;
☐ explained sufficiently how any proposed mitigation reduces the identified risk in question;
☐ evidenced our consideration of any less risky alternatives to achieving the same purposes of the processing, and why we didn't choose them;
☐ given details of stakeholder consultation (e.g. data subjects, representative bodies) and included summaries of findings;
☐ attached any relevant additional documents we reference in our DPIA, e.g. Privacy Notices, consent documents;
☐ recorded the advice and recommendations of our DPO (where relevant) and ensured the DPIA is signed off by the appropriate people;
☐ agreed and documented a schedule for reviewing the DPIA regularly or when we change the nature, scope, context or purposes of the processing;
☐ consulted the ICO if there are residual high risks we cannot mitigate.

How do we carry out a DPIA?
A DPIA should begin early in the life of a project, before you start your processing, and run alongside the planning and development process. It should include these steps:

You must seek the advice of your data protection officer (if you have one). You should also consult with individuals and other stakeholders throughout this process. The process is designed to be flexible and scalable. You can use or adapt the ICO's sample DPIA template.