CHESIL BANK
PARISH COUNCIL

Data Protection / Privacy Policy & Freedom of Information Policy

Adopted by full council:
Date: 14th May 2018
Updated:

Contents

1. Introduction

2. Statement of Policy

3. Privacy Policy

4. Data Protection Officer

5. Subject Access Request

6. Data Protection Impact Assessments

7. Cybersecurity

8. Security Incident Response

9. Freedom of Information Policy

10. Documents

1. Introduction

Chesil Bank Parish Council is fully committed to compliance with the requirements of the General Data Protection Regulation (GDPR) from 25th May 2018, which supersedes the Data Protection Act.
The Council will therefore follow procedures that aim to ensure that all employees, elected members, contractors, agents, consultants, partners or other servants of the council who have access to any personal data held by or on behalf of the council, are fully aware of and abide by their duties and responsibilities under the Act / Regulations and that the Council remains committed to protecting and respecting the privacy of all who provide their data.

For the purpose of the General Data Protection Regulation, the data controller is:
Chesil Bank Parish Council, West Elworth Farm, Portesham, Weymouth, Dorset, DT3 4HF

2. Statement of Policy

In order to operate efficiently, the Parish Council has to collect and use information about people with whom it works. This may include members of the public, current, past and prospective employees, clients and customers, and suppliers. In addition, it may be required by law to collect and use information in order to comply with the requirements of central government. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means there are safeguards within the Act / Regulation to ensure this. The Parish Council regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between the council and those with whom it carries out business. The Parish Council will ensure that it treats personal information lawfully and correctly. Personal data may be processed on the basis that such processing is necessary for the performance of tasks carried out by public authority acting in the public interest, out of contractual necessity or on a lawful basis.

The Parish Council will seek the consent of individuals and companies to hold their personal data, where possible to do so. Records of those consenting will be kept.

Article 5 of the General Data Protection Regulation requires that personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- 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; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
- 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.

3. Privacy Policy

Chesil Bank Parish council is committed to protecting and respecting the privacy of everyone and of ensuring it is fully compliant under the General Data Protection Regulation.

This policy (together with any other documents referred to within it) sets out the basis on which any personal data we collect, or is provided to us, will be processed. The following policy sets out the Parish Council's practices regarding the collection and processing of personal data and how we treat it.

a) Personal Data we may collect:

"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. 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 (GDPR) and other legislation relating to personal data and rights such as the Human Rights Act.

b) Data Controllers:

Chesil Bank Parish Council is the data controller for all data collected.

Other data controllers the council works with:

- Parish, District and County Councillors
- Local groups and organisations (Volunteers/Allotment holders)
- West Dorset District Council
- Dorset County Council
- HMRC and other Central Gov. bodies
- Charities
- Contractors

We may need to share personal data that 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 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 for the data. Where each of the parties listed above are processing data for their own independent purposes then each of us will be independently responsible.

c) What data do we process?

The council will process some, or all of, the following personal data where necessary to perform its tasks (see also the Parish Council's Information Audit):

- 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 venue, 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.

d) How we use sensitive personal data

- We may process sensitive personal data in order to comply with legal requirements and obligations to third parties.
- 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 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 an individual's interests and they are not capable of giving consent, or where the information is already public.

e) Do we need consent to process sensitive personal data?

- In limited circumstances, we may approach individuals for written consent to allow us to process certain sensitive personal data. If we do so, we will provide full details of the personal data that we would like and the reason we need it, so that the individual can carefully consider whether they wish to consent.

f) 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 and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have stated and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have stated.
- Kept and destroyed securely including ensuring that appropriate technical and security measures are in place to protect personal data from loss, misuse, unauthorised access and disclosure.

g) We use your personal data for some or all of the following purposes:

- To deliver public services, including to understand individuals needs to provide the services that they request and to understand what we can do for the individual and inform them of other relevant services;
- To confirm identity to provide some services;
- To contact 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; (see Safeguarding Policy).
- To promote the interests of the council;
- To maintain our own accounts and records;
- To seek views, opinions or comments;
- To notify of changes to our facilities, services, events and staff, councillors and other role holders;
- To send 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.

h) What is the legal basis for processing your personal data?

The council is a public authority and has certain powers and obligations. Most of the 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 the interests and rights of the individual. This Privacy Policy, and the Privacy Notices, we

display and distribute sets out the rights and the council's obligations to each individual. We may process personal data if it is necessary for the performance of a contract, or to take steps to enter into a contract. An example of this would be processing data in connection with the use of sports facilities, or the acceptance of an allotment garden tenancy. Sometimes the use of personal data requires consent, we will first obtain consent to use that data.

i) Sharing personal data

This section provides information about the third parties with whom the council may share personal data. These third parties have an obligation to put in place appropriate security measures and will be responsible to the individual directly for the manner in which they process and protect personal data. It is likely that we will need to share 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.

j) How long do we keep 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 8 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.

k) Individual rights and their personal data

Individuals have the following rights with respect to personal data:

When exercising any of the rights listed below, in order to process a request, we may need to verify identity for security. In such cases we will need the individual to respond with proof of identity before they can exercise these rights.

i) The right to access personal data we hold

- At any point an individual can contact us to request the personal data we hold 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 a 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.

ii) The right to correct and update the personal data we hold

- If the data we hold is out of date, incomplete or incorrect, individuals can inform us and the data will be updated.

iii) The right to have personal data erased

- If an individual feels that we should no longer be using their personal data or that we are unlawfully using it, they can request that we erase the personal data we hold.
- When we receive a 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).

iv) The right to object to processing of personal data or to restrict it to certain purposes only

- Individuals have the right to request that we stop processing their personal data or ask us to restrict processing. Upon receiving the request, we will contact the person concerned and let

them know if we are able to comply or if we have a legal obligation to continue to process the data.

v) The right to data portability

- Individuals have the right to request that we transfer some of their data to another controller. We will comply with a request, where it is feasible to do so, within one month of receiving it.

vi) The right to withdraw consent to the processing of data to which consent was obtained

- Individuals can withdraw their consent easily by telephone, email, or by post (see Contact Details below).

vii) The right to lodge a complaint with the Information Commissioner's Office.

- To lodge a complaint, individuals can contact the Information Commissioner's Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

l) 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.

m) Further processing

If we wish to use personal data for a new purpose, not covered by the Privacy Policy or Privacy Notice, then we will provide you 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 prior consent to the new processing.

n) Changes to the Policy

We keep this Privacy Policy under regular review and we will place any updates on the Parish Council's website at http://www.chesilbankparish.org/policiesandprocedures.html

4. Data Protection Officer - *Currently the Clerk is the Data Protection Officer but this is subject to confirmation from NALC and the ICO*

The Parish Council will appoint a Data Protection Officer (DPO), in line with the requirements of the GDPR. Currently the Clerk can The GDPR sets out in detail the minimum responsibilities of the Data Protection Officer ("DPO") role. GDPR specifies that DPOs "should assist the controller or the processor to monitor internal compliance with this Regulation".

The DPO's duties will include:

- informing and advising the council and its staff of their obligations in the GDPR and other data protection laws;
- monitoring compliance of the council, both in its practices and policies, with the GDPR and other data protection laws;
- raising awareness of data protection law; providing relevant training to staff and councillors;
- carrying out data protection-related audits;
- providing advice to the council, where requested, in relation to the carrying out of data protection impact assessments ('DPIAs') and the council's wider obligations with regard to DPIAs; and
- acting as a contact point for the Information Commissioner's Office.

As part of these duties to monitor compliance, the DPO may, in particular:

- collect information to identify processing activities;
- analyse and check the compliance of processing activities;
- inform, advise and issue recommendations to the controller or the processor;
- The appointed DPO must at all times have regard to 'the risk associated with the processing operations, taking into account the nature, scope, context and purposes of processing.' This is an overarching

obligation which means that the role of the DPO will vary in proportion to the risks to the rights of individuals affected by the council's processing of personal data.

- The DPO will 'cooperate with the supervisory authority, in the UK, this is the Information Commissioners Office ("ICO") and 'act as a contact point for the supervisory authority on issues relating to processing, and to consult, where appropriate, with regard to any other matter'.
- The controller or the processor, not the DPO, is required to 'maintain a record of processing operations under its responsibility' or 'maintain a record of all categories of processing activities carried out on behalf of a controller'.

The Data controllers and processors will ensure that:

- The DPO is invited to participate regularly in meetings of Officers and meetings of full council and relevant committee meetings.
- The DPO's name and contact details are provided to ICO;
- The DPO will be available to advise/ support councillors and relevant staff on data protection issues;
- The DPO will be present when decisions with data protection implications are taken;
- All relevant information will be passed on to the DPO in a timely manner in order to allow him or her to provide adequate advice;
- The opinion of the DPO will always be given due weight. In case of disagreement the Parish Clerk will document the reasons for not following the DPO's advice;
- The DPO will be promptly consulted once a data breach or another incident has occurred since the DPO will often have been involved in implementing data protection polices such as breach reporting and it will be important for the DPO to assess whether the policies work operationally.

5. Subject Access Request (SAR)

- The Parish Council will inform data subjects of their right to access data and provide an easily accessible mechanism through which such a request can be submitted.
- At any point an individual can contact us to request the personal data we hold 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 a 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.
- Ensure personal data is easily accessible at all times in order to ensure a timely response to SARs and that personal data on specific data subjects can be easily filtered.
- The Parish Council will implement standards to respond to SARs, including a standard response.

Upon receipt of a SAR the Parish Council will;

- Verify whether they are the controller of the data subject's personal data. If they are not the controller, but merely a processor, the Parish Council will inform the data subject and refer them to the actual controller.
- Verify the identity of the data subject; if needed, request any further evidence on the identity of the data subject.
- Verify the access request to ensure it is sufficiently substantiated. Ensure it is clear to the data controller what personal data is requested and If not request additional information.
- Verify whether requests are unfounded or excessive (in particular because of their repetitive character); if so, the Parish Council may refuse to act on the request or charge a reasonable fee.
- Promptly acknowledge receipt of the SAR and inform the data subject of any costs involved in the processing of the SAR.
- Verify whether you process the data requested. If you do not process any data, inform the data subject accordingly. At all times make sure the internal SAR policy is followed and progress can be monitored.
- Ensure data will not be changed as a result of the SAR. Routine changes as part of the processing activities concerned are permitted.
- Verify whether the data requested also involves data on other data subjects and make sure this data is filtered before the requested data is supplied to the data subject; if data cannot be filtered, ensure that other data subjects have consented to the supply of their data as part of the SAR.
- Respond to a SAR within one month after receipt of the request, If more time is needed to respond to complex requests, an extension of another two months will be taken, this will be communicated to the data subject in a timely manner within the first month;
- If the Parish Council cannot provide the information requested, it will inform the data subject on this decision without delay and at the latest within one month of receipt of the request.

- If a SAR is submitted in electronic form, any personal data will be provided by electronic means if possible.
- The Parish Council will include as a minimum the following information in the SAR response:
  - The purposes of the processing;
  - The categories of personal data concerned;
  - The recipients or categories of recipients to whom personal data has been or will be disclosed, in particular in third countries or international organisations, including any appropriate safeguards for transfer of data, such as Binding Corporate Rules or EU model clauses;
  - Where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period;
  - The existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
  - The right to lodge a complaint with the Information Commissioners Office ("ICO");
  - If the data has not been collected from the data subject: the source of such data;
  - The existence of any automated decision-making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
  - Provide a copy of the personal data undergoing processing.

Upon receipt of a SAR, the Clerk is to refer to the SAR Policy and templates provided by NALC saved under CBPC GDPR 2018.

6. Data Protection Impact Assessments (DPIAs)

The Parish Council will carry out Data Protection Impact Assessments, (DPIAs), when it is necessary. The decision to carry one out will be decided in consultation with the DPO whose advice will be sought in the following areas:

- Whether or not to carry out a DPIA;
- What methodology to follow when carrying out a DPIA;
- Whether to carry out the DPIA in-house or whether to outsource
- What safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects.
- Whether or not the data protection impact assessment has been correctly carried out and whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with the GDPR.
- If the Parish Council disagrees with the advice provided by the DPO, the DPIA documentation should specifically justify in writing why the advice has not been taken into account.
- The GDPR requires that councils carry out a DPIA when processing is likely to result in a high risk to the rights and freedoms of data subjects. This might include using CCTV to monitor public areas.

DPIA Assessment Checklist

Under the GDPR, data protection impact assessments (DPIAs) are mandatory where the processing poses a high risk to the rights and freedoms of individuals. While they can also be carried out in other situations, councils need to be able to evaluate when a DPIA is required. A checklist is provided by NALC to help Councils assess the need for a DPIA and provides a springboard for some of the issues to consider in more detail.

If two or more of the following apply, it is likely that a DPIA is required. This does not apply to existing systems but would apply if a new system is proposed.

1. Profiling is in use. Example: you monitor website clicks or behaviour and record people's interests. ☐
2. Automated-decision making. Example: when processing leads to the potential exclusion of individuals. ☐
3. CCTV surveillance of public areas. Processing used to observe, monitor or control data subjects. ☐
4. Sensitive personal data as well as personal data relating to criminal convictions or offences. ☐

5. Large scale data processing. There is no definition of "large scale". However consider: the number of data subjects concerned, the volume of data and/or the range of different data items being processed. ☐
6. Linked databases - in other words, data aggregation. Example: two datasets merged together, which could "exceed the reasonable expectations of the user" e.g. you merge your mailing list with another council, club or association. ☐
7. Data concerning vulnerable data subjects, especially when power imbalances arise, e.g. staff-employer, where consent may be vague, data of children, mentally ill, asylum seekers, elderly, patients. ☐
8. "New technologies are in use". E.g. use of social media, etc. ☐
9. Data transfers outside of the EEA. ☐
10. "Unavoidable and unexpected processing". For example, processing performed on a public area that people passing by cannot avoid. Example: Wi-Fi tracking. ☐

7. Cybersecurity

Data security is an ever-increasing risk for most organisations including councils. However, the number of breaches which are the result of highly sophisticated attacks from hackers is still very limited; most breaches are still the result of human error or relatively unsophisticated phishing attacks.

The main storage location for data is the Clerk's laptop (secure home office), memory sticks in locked storage at off site locations, where all users store data, and this is protected in the following way;

- Antivirus software
- Complex passwords of 8 or more characters secure all access
- Account lock out for 5 or more incorrect password in 30 minutes
- All email is stored in Google, which complies with Google data protection policies;

8. Security Incident Response

The Parish Council takes any breach of data security seriously and in the event of such a breach the following response plan will be followed:

A data security breach is defined as the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Examples of which are:

- Access by an unauthorised third party.
- Deliberate or accidental action (or inaction) by a controller or processor.
- Sending personal data to an incorrect recipient.
- Computing devices containing personal data being lost or stolen
- Loss of availability of personal data.

In the event of a breach the Clerk is to be notified immediately, and in her absence the Chairman should be informed. Clerk and Cllrs are instructed to report any breaches immediately they suspect one may have occurred. The DPO will then be consulted and an assessment will be made on the severity of any potential breach. Decisions are to be made by the Parish Clerk after consultation with the DPO and Cllrs. These decisions will include but are not limited to: notifying the correct supervisory bodies and the individual involved in the breach.

If after investigating the incident it is confirmed that a personal data breach occurred, we will establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it is likely that there will be a risk

then we will notify the Information Commissioners Office (ICO). Any notifications to the ICO will be done not later than 72 hours after the breach was identified. The GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. Article 34(4) allows us to provide the required information in phases, as long as this is done without undue delay. We will always prioritise the investigation, give it adequate resources, and expedite it urgently.

The Parish Clerk in conjunction with the Chairman or F & GP will decide if the breach is notifiable after assessing both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. In such cases, we will promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them, therefore allowing them time to take steps to protect themselves from the effects of a breach. We will provide them with the name and contact details of our DPO, a description of the likely consequences of the personal data breach; and what measures are being taken, or proposed to be taken, to deal with the breach and including, where appropriate, the measures taken to mitigate any possible adverse effects.

If the decision is taken not to notify individuals, we will still notify the ICO unless the breach is unlikely to result in a risk to rights and freedoms. However, if a decision is made not to inform the ICO then that decision will be documented. As with any other breach of procedures or security incident officers will thoroughly investigate to ascertain whether the breach was a result of human error or a systemic issue. It will then be determined the best way to ensure how a recurrence can be prevented, whether this is through better processes, further training or other corrective steps.

9. Freedom of Information Policy

The Council is committed to complying with the provisions of the Freedom of Information Act 2000 and associated legislation. This provides a general entitlement to information that the Council holds to any person subject to exemptions and conditions laid down by law.

Scope

This policy applies to all recorded information the Council holds regardless of how it was created or received. It applies regardless of the media the information is stored in whether the information may be on paper, held electronically or as an audio recording. The Act is fully retrospective. Dealing with requests the Parish Council offers advice and assistance to anybody who wishes to make a Freedom of Information (FOI) request. The Council is committed to dealing with requests within the statutory timescales of no more than 20 working days. This can be extended in specific circumstances on legal advice. However, the Council is committed to providing a prompt service.

The Council will claim exemptions as appropriate whilst maintaining a commitment to openness, scrutiny and the public interest and will inform the FOI applicant when exemptions have been applied. Where appropriate, requests in writing will be treated as Freedom of Information requests. There is no need for requests to indicate they are made under the Act. The Council reserves the right to refuse requests where the cost of supply of the information would exceed the statutory maximum (see section 12 of the Act.).

Adopting and Maintaining Publication Schemes

The Council has adopted an Information Publication Scheme (attached at Appendix A) and is committed to updating and maintaining it to keep it current and relevant. The Publication Scheme contains many of the documents, policies, plans and guidance which are usually asked for and much more. Material contained within the publication scheme, and a copy of the scheme itself, is readily available. Where charges are applied these are stated in the Scheme. The scheme can also be accessed via the website. The Parish Clerk will give advice and assistance on how to use the scheme as appropriate. This scheme is reviewed an updated on an annual basis.

Responsibilities

The Parish Clerk is responsible for ensuring that any request for information is dealt with under the Act and in compliance with this policy. The Clerk is also responsible for good information handling practice and implementing records management policies and procedures as appropriate. The Council will carefully consider its responsibilities under GDPR before releasing any personal data about living individuals, including current and former officers, current and former Council Members, and users of the Council's services.

Contact Details
For advice and assistance please contact the Parish Council:

Chesil Bank Parish Council
West Elworth Farm, Portesham
Weymouth, Dorset
Tel: 07814 016971
Email: theclerk@chesilbankparish.org
Website: www.chesilbankparish.org.

Further advice and information, including a full list of exemptions and advice on the public interest test, is available from the Information Commissioner's Office www.ICO.org.uk.

10. Associated Documents

Other documents related to both the Data Protection and Freedom of information policy are:
- Model Publication Scheme (attached at Appendix A)
- Risk Management Policy (including Financial)
- Privacy Notice
- Audit Questionnaire
- Information Audit

Appendix A

Information available from Chesil Bank Parish Council

Information to be published	Location	Comments
Class 1 – Who we are and what we do		
Location of main Council office and accessibility details	Clerks' Home Office	Agendas, reports and minutes are also published online and available to view for one year before they are archived.
Contact details for Parish Clerk	1 , 4, & 5	
List of Councillors representing each ward (incl. address and telephone no.)	1, 2, 3 & 5	
Membership of Working Groups	1 & 5	
Chesil Bank Code of Conduct	1 & 5	
Agendas (last 2 years)	1 & 5	
Reports to Council (last 2 years)	1 & 5	
Minutes of Council (last 2 years)	1 & 5	
Standing Orders	1 & 5	
Terms of Reference for Working groups	1	
Council's Parish Plan 2010	1 & 5	
Guidelines for Parish Councillors appointed as representatives to community and local organisations	1 & 5	
Emergency Telephone Numbers	1 & 5	
Exclusions – Confidential Agendas, Minutes and Reports (pre-2007 or staff related). This is where the documents contain exempt information. Typically information may be withheld if it is personal data and its disclosure would contravene the General Data Protection Regulations or if the information relates to legal proceedings or advice, or if disclosure would prejudice the commercial interests of another person. Since 2007 confidential Minutes other than those relating to staff are released into the public domain with the public minutes.		
Class 2 – What we spend and how we spend it		
Current and previous financial year as a minimum	1 & 5	Previous years- 2

Annual return form and report by auditor – internal and external (limited to the last financial year)	1 2 & 5	
Budgets	1	
Precept request (limited to the last financial year)	1	
VAT records (limited to the last financial year)	1 & 2	Previous 6 years – 2
Financial Standing Orders and Regulations (including those dealing with the award of contracts)	1, 2 & 5	
Grants Criteria	1 & 5	
- Grants given and received are minuted in the Finance & Staffing Committee Minutes	1	
Service Level Agreements and Contracts	1 & 2	(under subject title)
Members' allowances and expenses	1	
Fees and charges applied by the Council	1	Previous years – 2
Receipt/Payment records, receipt books of all kinds, bank statements from all accounts (limited to the last financial year)	Current year – 1 & 2	Previous 6 years – 2
Purchase of goods/services £100 and over	Monthly & 5	Produced annually
Exclusions – All commercially sensitive information e.g. quotations and tenders, loan documentation and insurance policies. With regard to quotations and tenders, this information is treated as confidential to ensure that the whole tender process is fair i.e. if tender information is released to a third party prior to the end of the tender period those who initially submitted tenders could be undercut and or unfairly disadvantaged.		
Class 3 – What our priorities are and how we are doing Strategies and plans, performance indicators, audits, inspections and reviews		
Parish plan 2010	1, 2 & 5	
Risk Assessments	1 & 2	
Neighbourhood Plan Project	NA	
Annual Report to Parish or Community Meeting (current and previous year as a minimum)	NA	
Quality Status	NA	
Best Value Performance Plan	N/A to CBPC	

Best Value Inspection Reports	N/A to CBPC	
Class 4 – How we make decisions Decision making processes and records of decisions, current and previous council year as a minimum		
Timetable of meetings (Council, any working group meetings and parish meetings)	1 & 5	
Agendas of meetings (as above)	1 & 5	
Minutes of meetings (as above) – nb this will exclude information that is properly regarded as private to the meeting.	1	
Reports presented to council meetings - nb this will exclude information that is properly regarded as private to the meeting.	1	
Responses to consultation papers	1	
Analysis of responses received to public consultations by the Council	1 & 5	
Public consultations with local community	1 & 5	
Bye-laws	NA	
Responses to planning applications	1, 5 & WDDC planning	
Exclusions – Copies of planning consultations, the Development Plan, Structure Plan, Local Plan and Rights of Way/Footpath maps all of which are available from the local planning and/or highway authority respectively.		
Class 5 – Our policies and procedures Current written protocols, policies and procedures for delivering our services and responsibilities		
<u>Policies and procedures for the conduct of council business</u>: Policy statements issued by the Council Standing orders Working Group terms of reference Delegated authority in respect of officers Code of Conduct Safety Inspection Records	1 & 5 1 & 5 1 & 5 1 NA 1 & 5 1 & 2	

Health & Safety Policy	1 & 5	
<u>Policies and procedures for the provision of services and about the employment of staff:</u> Internal policies relating to the delivery of services Equality and diversity policy Health and safety policy Recruitment policies (including current vacancies) Job Descriptions Terms and Conditions of Employment Policies and procedures for handling requests for information (this document will be held in reception) Complaints procedures (including those covering requests for information and operating the publication scheme) Staffing Structure	 1 NA 1 NA 1 1 & 2 1 & 2 1 & 5 1	
Information security policy	1	
Records management policies (records retention, destruction and archive)	1 & 5	
Data protection policies	1 & 5	
Schedule of charges (for the publication of information)	1 & 5	
Exclusions - all personal records i.e. appraisals, employee specific salary details, disciplinary records, sickness records and the like by virtue of being personal data under the Data Protection Act 1988.		
Class 6 – Lists and Registers Currently maintained lists and registers only		
Any publicly available register or list (if any are held this should be publicised; in most circumstances existing access provisions will suffice)	1	
Information relating to the last periodic electoral review of the council area	1 / WDDC	
Information relating to the latest boundary review of the council area	1 / WDDC	

Assets Register	1 2 & 5	
Disclosure log (indicating the information that has been provided in response to requests; recommended as good practice, but may not be held by parish councils)	N/A to CBPC	
Register of gifts and hospitality	1	
Members' Declaration of Acceptance of Office	1 & 5	
Register of Members' Attendance and Pecuniary and Personal Interests	1	
Class 7 – The services we offer (Information about the services we offer, including leaflets, guidance and newsletters produced for the public and businesses) Current information only (hard copy or website; some information may only be available by inspection)		
Allotments	1 &5	
- Standard Tenancy Agreements	1 & 5	
Exclusion – Individual tenancy agreements and rent payment records under both privacy and data protection laws.		
Burial grounds and closed churchyards	1 & 5	
- Plans of Cemetery	1 & 5	
- Pricing Policies / General Policies	1 & 5	
Exclusion – All documentation relating to individual applications and registrations under both privacy and data protection laws.		
CCTV & ANPR Privacy Impact Assessments	NA	
Parks, playing fields and recreational facilities	1	
Seating, litter bins, memorials etc	1	
Bus shelter	1	
Public conveniences	NA	
Agency agreements	1	
A summary of services for which the council is entitled to recover a fee, together with those fees (e.g. burial fees)	NA	

Additional Information This will provide Councils with the opportunity to publish information that is not itemised in the lists above		
Events Guide	NA	
Venues for Hire Guide	1 & 5	
Tourist Information	NA	
Parish, community guide	NA	
Parish Council Newsletters	NA	
History Books on Chesil Bank	History Centre Dorchester	

CONTACT DETAILS: **Parish Clerk**, Chesil Bank Parish Council, West Elworth Farm, Portesham, Weymouth, Dorset, DT3 4HF

KEY TO LOCATIONS IN THE PARISH CLERK'S OFFICE

(1) PC Laptop/Memory Sticks
(2) Filing Cabinet (Offsite storage cupboard)
(3) Filing Cabinet (At Clerk's secure home Office)
(4) Facebook
(5) Parish Council's Website

SCHEDULE OF CHARGES

TYPE OF CHARGE	DESCRIPTION	BASIS OF CHARGE
Disbursement cost	Photocopying @ 8p per sheet (black & white)	0.86p (actual cost incurred by CBPC) + VAT
	Postage	Actual cost of Royal Mail standard 2nd class

Any charges made by Chesil Bank Parish Council for routinely published material must be justified and transparent and kept to a minimum. Material which is published and accessed on a website will be provided free of charge. Charges may be made for actual disbursements incurred such as photocopying and also a postage charge if you are unable to call into the office to collect them. The cost will be 8p per page plus actual postal charges. If a charge is to be made, the individual will be informed of the charge and why it is to be incurred prior to the information being provided. Payment may be requested prior to release of the information. Charges may also be made for information provided under the scheme where it is legally authorised. Any subject access requests to information will be complied within one month. Your request will be refused or charged for if it is manifestly unfounded or excessive.