

MELLS PARISH COUNCIL

General Data Protection Regulation Policies

(Adopted 11 August 2026)

Index

Information and Data Protection Policy	Page 2
Privacy notice	Page 8
Management of transferable data policy	Page 10
Data privacy impact assessment	Page 15
Data security incident procedure	Page 20
Consent to hold contact information	Page 23
Subject access request form	Page 25

Contact information

Mells Parish Council

clerk@mellsparishcouncil.gov.uk

Tel: 07704 854953

Information Commissioner's Office

casework@ico.org.uk

Tel: 0303 123 1113.

INFORMATION & DATA PROTECTION POLICY

Introduction

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

Mells 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.

This Policy is linked to our ICT Policy which will ensure information considerations are central to the ethos of the organisation.

Mells 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.

Mells Parish 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

Mells 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 it, seek to strike a balance between the rights of individuals and the sometimes, competing interests of those such a Mells 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 Mells 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. Mells 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.

Mells 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 Mells Parish 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?

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

Diversity Monitoring

Mells Parish Council monitors 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.

Mells Parish 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 Mells 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.

Mells Parish Council's 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 Mells Parish Council.

Information Security

Mells 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 our Parish Clerk.

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: Parish Clerk.

Information Deletion: If the individual wishes Mells 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.

Mells 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 or the Information Commissioners Office casework@ico.org.uk Tel: 0303 123 1113.

Mells Parish Council will always give guidance on personnel data to employees through the Employee handbook.

Mells Parish 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 Mells Parish 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 Mells Parish 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 Mells Parish Council will make available and hopefully make it easier for people to access it.

All formal meetings of Mells Parish Council and its committees are subject to statutory notice being given on notice boards, the Website and sent to the local media. Mells Parish 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. Mells Parish Council welcomes public participation and has a public participation session on each Mells Parish Council and committee meeting. Details can be seen in Mells Parish Council's Standing Orders, which are available on its Website.

Occasionally, Mells Parish 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.

Mells Parish 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

Mells Parish 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

Mells Parish 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 in-formation.

“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.

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.

Mells Parish Council's 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

Mells 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 Mells 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 Data Information Officer: Miss J Book (contact details above).

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: Miss J Book (contact details above) to request this.

Information Deletion

If you wish Mells Parish Council to delete the information about you please contact: Miss J Book (contact details above) 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 Miss J Book (contact details above) to object.

Rights Related to Automated Decision Making and Profiling

Mells 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 pro-filing, 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 Mells Parish Council Data Information Officer: Joy Book (contact details above) and the Information Commissioners Office casework@ico.org.uk Tel: 0303 123 1113.

THE MANAGEMENT OF TRANSFERABLE DATA POLICY

Contents

Purpose
Principals
Advice and assistance
Responsibilities
Incident management
Data administration
Security
Use of removable media
Faulty or unneeded storage devices
Breach of procedures
Review and revision
Employees guide in brief

Purpose

- 1.1 This policy supports the controlled storage and transfer of information by Councillors and all employees, temporary staff and agents (contractors, consultants and others working on behalf of Mells Parish Council) who have access to and use of computing equipment that is owned or leased by Mells Parish Council
- 1.2 Information is used throughout Mells Parish Council and is sometimes shared with external organisations and applicants. The use of removable media may result in the loss of the ability to access information, or interference with the integrity of information, which could have a significant effect on the efficient operation of Mells Parish Council and may result in financial loss and an inability to provide services to the public.
- 1.3 It is therefore essential for the continued operation of Mells Parish Council that the availability, integrity and confidentiality of all storage devices are maintained at a level which is appropriate to the Council's needs.
- 1.4 The aims of the policy are to ensure that the use of removable storage devices is accomplished with due regard to:
 - 1.4.1 Enabling the correct data to be made available where it is required
 - 1.4.2 Maintaining the integrity of the data
 - 1.4.3 Preventing unintended consequences to the stability of the computer network
 - 1.4.4 Building confidence and trust in data that is being shared between systems
 - 1.4.5 Maintaining high standards of care towards data and information about individual parishioners, staff or information that is exempt from disclosure
 - 1.4.6 Compliance with legislation, policies or good practice requirements

2 Principals

- 2.1 This policy sets out the principles that will be adopted by Mells Parish Council in order for material to be safely stored on removable media so that the risk of loss or corruption to work data is low.
- 2.2 Removable media includes but is not limited to:
USB memory sticks, memory cards, portable memory devices, CD / DVDs, diskettes and any other device that transfers data between systems, or stores electronic data separately from email or other applications.
- 2.4 Any person who intends to store Council data on removable media must abide by this Policy. This requirement devolves to Councillors, employees and agents of Mells Parish Council, who may be held personally liable for any breach of the requirements of this policy.
- 2.5 Failure to comply with this policy could result in disciplinary action.

3 Advice and Assistance

- 3.1 The clerk will ensure that everyone that is authorised to access Mells Parish Council's information systems is aware of their obligations arising from this policy.
- 3.2 A competent person should be consulted over any hardware or system issues. Advice and guidance on using software packages should be also sort from a competent person.

4 Responsibilities

- 4.1 Clerks are responsible for enforcing this policy and for having arrangements in place to identify the location of all data used in connection with Mells Parish Council business.
- 4.2 Users of removable media must have adequate Records Management / Information Security training so that relevant policies are implemented.

5 Incident Management

- 5.1 It is the duty of all employees and agents of Mells Parish Council to not allow storage media to be compromised in any way whilst in their care or under their control. There must be immediate reporting of any misuse or irresponsible actions that affect work data or information, any loss of material, or actual, or suspected breaches in information security to the clerk.
- 5.2 It is the duty of all Councillors/Employees to report any actual or suspected breaches in information security to the clerk.

6 Data Administration

- 6.1 Removable media should not be the only place where data created or obtained for work purposes is held, as data that is only held in one place and in one format is at much higher risk of being unavailable through loss, destruction or malfunction of equipment, than data which is routinely backed up.

- 6.2 Where removable media is used to transfer material between systems then copies of the data should also remain on the source system or computer, until the data is successfully transferred to another computer or system.
- 6.3 Where there is a business requirement to distribute information to third parties, then removable media must only be used when the file cannot be sent or is too large to be sent by email or other secure electronic means.
- 6.4 Transferring material to removable media is a snapshot of the data at the time it was saved to the media. Adequate labelling must be undertaken so as to easily identify the version of the data, as well as its content.
- 6.5 Files must be deleted from removable media, or the removable media destroyed, when the operational use of the material has been completed. Mells Parish Council's retention and disposition schedule must be implemented by Councillors, employees, contractors and agents for all removable media.

7 Security

- 7.1 All storage media must be kept in an appropriately secure and safe environment that avoids physical risk, loss or electrical corruption of the business asset. Due to their small size there is a high risk of the removable media being mislaid lost or damaged, therefore special care is required to physically protect the device and the data. Anyone using removable media to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.
- 7.2 Virus Infections must be prevented from damaging Mells Parish Council's network and computers. Virus and malware checking software approved by Mells Parish Council, must be operational on both the machine from which the data is taken and the machine on to which the data is to be loaded. The data must be scanned by the virus checking software, before the media is loaded on to the receiving machine.
- 7.3 Any memory stick used in connection with Mells Parish Council equipment or to store Council material should usually be Mells Parish Council owned. However work related data from external sources can be transferred to the Council network using memory sticks that are from trusted sources and have been checked using current anti-virus software.
- 7.4 Mells Parish Council will not provide support or administrator access for any non-council memory stick.

8 Use of removable media

- 8.1 Care must be taken over what data or information is transferred onto removable media. Only the data that is authorised and necessary to be transferred should be saved on to the device.
- 8.3 Council material belongs to Mells Parish Council and any equipment on which it is held should be under the control of Mells Parish Council and not available to be used for other purposes that may compromise the data.

- 8.4 All data transferred to removable media should be in accordance with an agreed process established by Mells Parish Council so that material can be traced.
- 8.5 The person arranging the transfer of data must be authorised to make use of, or process that particular data.
- 8.6 Whilst in transit or storage the data must be given appropriate security according to the type of data and its sensitivity.
- 8.7 Encryption must be applied to the data file unless there is no risk to Mells Parish Council, other organisations or individuals from the data being lost whilst in transit or storage. If encryption is not available then password control must be applied if removable media must be used for the business purpose.

9 Faulty or Unneeded Storage Devices

- 9.1 Damaged or faulty media must not be used. The clerk must be consulted over any damaged equipment, peripherals or media.
- 9.2 All unneeded or faulty storage devices must be dealt with securely to remove the data before reallocating or disposing of the device.

10 Breach procedures

- 10.1 Users who do not adhere to this policy will be dealt with through Mells Parish Council's disciplinary process.
- 10.2 Where external service providers, agents or contractors breach the policy, this should be addressed through contract arrangements.

11 Review and Revision

- 11.1 This policy will be reviewed annually by Mells Parish Council and revised according to developments in legislation, guidance, accepted good practice and operational use.

12 Employees Guide in Brief

- 12.1 Data and information are valuable and must be protected.
- 12.2 Only transfer data onto removable media, if you have the authority to do so.
- 12.4 All transfer arrangements carry a risk to the data.
- 12.5 Run the virus checking programme on the removable media each time it is connected to a computer.
- 12.6 Only use approved products for Mells Parish Council data.
- 12.7 Activate encryption on removable media wherever it is available and password protection if not available

Data should be available for automatic back up and not solely saved to removable media.

- 12.8 Delete files from removable media, or destroy the media, after the material has been used for its purpose.

DATA PRIVACY IMPACT ASSESSMENT

Screening Questions

These questions are intended to help you decide whether a DPIA is necessary. Answering 'yes' to any of these questions is an indication that a DPIA would be necessary. You can expand on your answers as the project develops if you need to.

Question	Response
Will the project involve the collection of new information about individuals?	☐ Yes ☐ No
Will the project compel individuals to provide information about themselves?	☐ Yes ☐ No
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	☐ Yes ☐ No
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	☐ Yes ☐ No
Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics, or CCTV.	☐ Yes ☐ No
Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?	☐ Yes ☐ No
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 very private.	☐ Yes ☐ No

Will the project require you to contact individuals in ways that they may find intrusive?	☐ Yes ☐ ☐ No
---	---

Step One – Why you are conducting a DPIA

Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties. You may find it helpful to link to other relevant documents related to the project, for example a project proposal. Also summarise why the need for a PIA was identified (this can draw on your answers to the screening questions).

Step Two – Describe the information involved

You should describe the collection, use and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of data flows. You should also state how many individuals are likely to be affected by the project.

Step Three – Identify the privacy and related risks

Principle 1 – Lawfulness, fairness and transparency

Privacy Issue	Comment
Have you identified the purpose of the project?	
How will you tell individuals about the use of their personal data?	
Do you have a Privacy Notice in place to cover the processing of this data?	
If so does it need to be updated?	
Please tick the data items collected. Personal	☐ Name ☐ Next of Kin ☐ Date of Birth ☐ Sex ☐ Address ☐ Post Code ☐ National Insurance Number

Sensitive	☐ Sexual Orientation ☐ Political Opinions ☐ Religion ☐ Physical or Mental Health ☐ Ethnic Origin
	☐ Union Membership ☐ Genetic / Biometric Other (please state):
Who provides the information?	
Have you established the legal basis for processing? If so, what is it?	
If you are relying on consent to process personal data, how will this be collected and recorded?	
Do you need to validate the age of the data subject and if so how will this be done?	
Have you checked and confirmed that the data subject has capacity to give consent?	

Principle 2 – Purpose limitation

Privacy Issue	Comment
Please state the purpose for the processing of the data: (e.g. research, audit, service provision)	
Which personal data will you not need to use without compromising the needs of the service/project?	

Principle 3 – Data minimisation

Privacy Issue	Comment
Will you only collect personal data actually needed for the specified purposes of the service/project?	

Are you procuring software that will allow you to delete information in line with your retention periods?	
How will the data be destroyed when it is no longer required?	

Principle 4 – Accuracy

Privacy Issue	Comment
How are you ensuring that the personal data obtained from individuals or other organisations is accurate?	
How will the information be kept up to date and checked for accuracy and completeness?	
If the data subject withdraws their consent how will this be actioned and recorded?	
Is there a documented process to amend and/or delete data when necessary?	

Principle 5 – Storage limitation

Privacy Issue	Comment
What personal data will be held and why are you holding it?	
What is the retention period to hold personal data?	
Is there a policy with standard retention periods in place?	
Will the personal data information to be held be regularly reviewed and erased or anonymise when no longer needed?	
Is there an appropriate processes in place to comply with individuals' requests for erasure under 'the right to be forgotten'.	
Will personal data be clearly identified that you will need to keep for public interest archiving, scientific or historical research, or statistical purposes?	

Principle 6 – Integrity and confidentiality (security)

Privacy Issue	Comment
Do the systems provide protection against the security risks identified?	
What training and /or guidance is in place to ensure that staff know how to operate the system securely?	
Is there an audit trail in place for the system/asset?	
Where will the information be kept/stored/accessed?	
Will any information be sent off site? If yes where will it be sent and how will it be transferred?	
Is there an access policy in place which covers the data referred to in the DPIA?	
Is there a contingency plan/back up policy in place to manage the effect of an unforeseen event?	
Are there procedures in place to recover data (both electronic and paper) which may be damaged through human error, computer virus, network failure, theft, fire or flood?	

Principle 7 – Accountability

Privacy Issue	Comment
Will you have appropriate measures and records in place to be able to demonstrate your compliance with the principles of the Data Protection Act 2018?	

Step 4 – Completion of Risk Assessment and Mitigation

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm Remote, possible or probable	Severity of harm Minimal, significant or severe	Overall risk Low, medium or high

Step 5 – Sign off and record of DPIA outcomes

<u>Risks</u>	<u>Approved Solution</u>	<u>Approved by</u>	<u>Date Approved</u>

DATA SECURITY INCIDENT PROCEDURE

1. Introduction

- 1.1 The Council has a responsibility to ensure that personal information is kept and used securely. If anything goes wrong and, for example, data is lost, stolen, misused, sent to the wrong address or inappropriately accessed or released, the Council has a responsibility to put things right.
- 1.2 All suspected information security incidents must be reported to the Data Lead. This enables the Data Lead to conduct a full investigation, and to identify areas of weakness and improvements that need to be made. It also enables the Data Lead to take a decision as to whether the incident should be reported to the Information Commissioner's Office as a data breach. The latter must be done within 72 hours of discovery, therefore all suspected incidents must be reported to the Data Lead as soon as they are discovered.
- 1.3 When sensitive information has been put at risk, but has not actually been lost, stolen, misused or inappropriately accessed or released, it may not be an incident requiring re-reporting to the Information Commissioner's Office however it is not good practice. For example, a member of staff taking sensitive information home without authority but re-turning it safely the next day would have put data at risk. The Data Lead will still put measures in place to prevent a reoccurrence.
- 1.4 All staff and councillors must be made aware of this procedure.

2. Procedure

- 2.1 All identified incidents must be reported to the Data Lead as soon as they are detected. Even where there is some difference of opinion regarding breach, err on the side of caution and report it.
- 2.2 Upon detecting a breach, it is important to act quickly. In particular it is important to let the Data Lead know the following:
 - The extent of the breach
 - The amount of information involved
 - The sensitivity of information involved
- 2.3 The Data Lead will investigate the incident and establish why it happened, whether or not it constitutes a breach and what remedial action is necessary.
- 2.4 The Data Lead will use their initial assessment to report the breach if it meets the necessary threshold for reporting to the Information Commissioner's Office within 72 hours of the discovery of the breach. If this is done after 72 hours, the Data Lead will provide an explanation for this.
- 2.5 The Data Lead will prepare an incident report containing the following:
 - A timeline of dates and times concerning the incident
 - The potential for loss or damage to individuals, the parish council or any other body
 - What measures need to be taken and how quickly to address:-
 - i. Restoring any lost information to our custody or control

- ii. Whether to warn people about the loss, including who to warn and when. This may require a risk assessment.
 - iii. Factors taken into account for deciding to report the loss to the Information Commissioner's Office.
 - iv. Whether to report the loss to the Police.
- 2.6 The Data Lead will consider taking statements from those involved, especially where the quality of evidence may be lost through time or people may not be present for long.
- 2.7 The Data Lead will report any actions that need to be taken to prevent a reoccurrence of the breach and the parish council will ensure that these are implemented.
- 2.8 The Data Lead will write to any data subject(s) affected, if necessary dependant on the outcome of a risk assessment, and deal with any subsequent complaint. A standard letter template for this is in Appendix 1.
- 2.9 The Data Lead will also correspond as applicable with any member of the public reporting a breach.
- 2.10 The Data Lead will deal with any correspondence from the Information Commissioner's Office, providing any further information requested and implementing any recommendations.

Letter to notify that personal data has been breached

I write to you to bring to your attention a breach of the Data Protection Act that unfortunately involves your personal data.

As you would imagine we have taken this matter very seriously and *are investigating the matter / have concluded our investigation into it.*

The facts in this matter are *<give brief description of what has happened, eg a letter intended for you was sent to another individual because of an administrative error. The other individual immediately notified me on receipt and returned the letter.>.*

I am unable for reasons of confidentiality to go into details of my investigation, however I am able to tell you that you *<state what remedial action(s) have been carried out / what has been to prevent a reoccurrence, without breaching confidentiality>*

If you have any questions or concerns regarding this letter, please get in touch with me *or alternatively speak to your social worker who is aware of the situation.*

I would again like to apologise for the incident of which you were no doubt unaware.

Yours sincerely,

GENERAL DATA PROTECTION REGULATION (SERVICE)

CONSENT TO HOLD CONTACT INFORMATION

I agree that I have read and understand Mells Parish Council's Privacy Notice. I agree by signing below that the Council may process my personal information for providing information and corresponding with me.

I agree that Mells Parish Council can keep my contact information data for an undisclosed time or until I request its removal.

I have the right to request modification on the information that you keep on record.

I have the right to withdraw my consent and request that my details are removed from your database.

Name	
Date of birth if under 18	
Parental/Guardian Consent for any data processing activity	
Address	
Telephone No.	
Email Address	
Facebook	
Signature	
Date	

For office use only:

Guidance Notes Data Sharing Checklist – systematic data sharing

Scenario: You want to enter into an agreement to share personal data on an ongoing basis is this form relevant and the sharing justified? Read the below:

Key points to consider:

What is the sharing meant to achieve?

Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?

- Is the sharing proportionate to the issue you are addressing?
- Could the objective be achieved without sharing personal data?

Do you have the power to share?

Key points to consider:

- The type of organisation you work for.
- Any relevant functions or powers of your organisation.
- The nature of the information you have been asked to share (for example was it given in confidence?).
- Any legal obligation to share information (for example a statutory requirement or a court order).

If you decide to share

It is good practice to have a data sharing agreement in place.

As well as considering the key points above, your data sharing agreement should cover the following issues:

- What information needs to be shared?
- The organisations that will be involved.
- What you need to tell people about the data sharing and how you will communicate that information.
- Measures to ensure adequate security is in place to protect the data.
- What arrangements need to be in place to provide individuals with access to their personal data if they request it?
- Agreed common retention periods for the data.
- Processes to ensure secure deletion takes place.

Date Data re- ceived	Date consent re- ceived and ap- proved for data to be held	Data received as Phone, email, hard copy or other	Data ap- proved to be shared with the below	Removal of consent re- ceived	Date data dis- posed of and method of disposal ac- tioned

SUBJECT ACCESS REQUEST FORM

Under the Data Protection Act you have a statutory right to request confirmation that the council is processing your data and to request to see information held on you by that organisation.

You also have the right to be told:

- the purposes of and legal basis for the processing;
- the categories of personal data concerned;
- the recipients or categories of recipients to whom the personal data has been disclosed;
- the period for which the personal data is to be held;
- that you have rights to rectification and erasure of personal data where, for example, factual information has been recorded incorrectly;
- that you have the right to lodge a complaint with the Information Commissioner's Office and the contact details of the Commissioner;
- any information about the origin of the personal data concerned.

This information is likely to be available in general terms within our privacy notices, however you can request it in addition to any request to see your records.

To request to see your records, please complete this form, read and sign the declaration and then send the completed form to the Parish Clerk, Mells Parish Council, by email

parshclerk@Mellsparishcouncil.gov.uk or contact the Parish Clerk on 07704 584953.

To ensure proper security, the Council must be sure of your identity before complying with a subject access request. To confirm your identity, we need to see an official document with a photograph, such as a driving licence or a passport.

If you are making the request on behalf of another individual to access their information, we will need written consent from the individual to whom the data relates as well as your proof of identity. If you have legal authorisation to act on behalf of an individual, such as if you act with power of attorney or as a litigation friend, you will need to provide a copy of that authorisation to evidence it.

We can refuse your request if it is manifestly unfounded or excessive, such as if it is repetitive. We will explain why we consider your request to be manifestly unfounded or excessive if we do refuse it.

1. Details of the person making the request	
Title:	
First name(s):	
Surname:	

Any other names that you have been known by	
Date of Birth:	
Address:	
Daytime telephone number:	
Email address:	

2. Are you requesting information about yourself?	
If Yes	Please go to section 4
If No	If you are making the request on behalf of another person you must enclose with the request a signed authority from them to do so. If you are making the application because the data subject lacks capacity to make the application in their own right please outline your authority to make the application in their stead (for example, Power of Attorney). You should enclose a copy of any evidence that you may have of that authority. The Council will contact you if further evidence is required. (please complete section 3)

3. Details of the Data Subject (if requesting information on behalf of someone else)	
Title:	
First name(s):	
Surname:	
Date of Birth:	

Address:	
----------	--

Daytime telephone number:	
Email address:	
Relationship to Data Subject	

4. Describe the information you are requesting.

If you are only seeking certain records, it would be helpful for us to know which types of record you are seeking, any time period to cover, and if you would like to see only specific document(s). Please describe these below with as much detail as you can.

Declaration:

I certify that the information given on this form is true and correct.

Signed:

Date:

Return Address

Parish Clerk
Mells Parish Council
07704 584953
clerk@mells-pc.gov.uk

If as a result of the response to your request you are dissatisfied with the way we are using your personal information you should raise the matter with the Data Protection Officer who can be contacted via the address above. We will do everything we can to put the matter right if the council has not processed your data correctly. You also have a right to make a complaint about our handling of your personal data to the Information Commissioner's Office, whose web site is <https://ico.org.uk/>

We only use the information that you provide for us to process your request. We may need to share that you have made a request with other organisations if we hold information about you that they have supplied and we need to consult with those organisations regarding release of the information to you. Records of requests will be kept for 6 years after the closure of the request for operational, statistical and audit purposes.

Signed: _____

Date: _____

Position: _____