Horton Parish Council

Assertion 10 compliance documents 2026

Data Protection Policy

Privacy Notice

Document Retention Policy

IT policy

Email Policy

Website accessibility Statement

Data Breach Policy

Data Breach reporting form

Freedom of Information Policy

Publication Scheme

GDPR Map

HORTON PARISH COUNCIL DATA PROTECTION POLICY

Purpose

The council is committed to being transparent about how it collects and uses the personal data of staff, and to meeting our data protection obligations. This policy sets out the council's commitment to data protection, and your rights and obligations in relation to personal data in line with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA).

This policy applies to the personal data of current and former job applicants, employees, workers, contractors, and former employees, referred to as HR-related personal data. This policy does not apply to the personal data relating to members of the public or other personal data processed for council business.

The council has appointed Zannette Bougourd – Parish Clerk and RFO as the person with responsibility for data protection compliance within the council. Questions about this policy, or requests for further information, should be directed to them.

Definitions

"Personal data" is any information that relates to a living person who can be identified from that data (a ‘data subject’) on its own, or when taken together with other information. It includes both automated personal data and manual filing systems where personal data are accessible according to specific criteria. It does not include anonymised data.

“Processing” is any use that is made of data, including collecting, recording, organising, consulting, storing, amending, disclosing or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic or biometric data as well as criminal convictions and offences.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Data protection principles

The council processes HR-related personal data in accordance with the following data protection principles the council:

- processes personal data lawfully, fairly and in a transparent manner
- collects personal data only for specified, explicit and legitimate purposes
- processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing

- keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay
- keeps personal data only for the period necessary for processing
- adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage

The council will tell you of the personal data it processes, the reasons for processing your personal data, how we use such data, how long we retain the data, and the legal basis for processing in our privacy notices.

The council will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it. The council will not process your personal data if it does not have a legal basis for processing.

The council keeps a record of our processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

Processing

Personal data

The council will process your personal data (that is not classed as special categories of personal data) for one or more of the following reasons:

- it is necessary for the performance of a contract, e.g., your contract of employment (or services); and/or
- it is necessary to comply with any legal obligation; and/or
- it is necessary for the council's legitimate interests (or for the legitimate interests of a third party), unless there is a good reason to protect your personal data which overrides those legitimate interests; and/or
- it is necessary to protect the vital interests of a data subject or another person; and/or
- it is necessary for the performance if a task carried out in the public interest or in the exercise of official authority vested in the controller.

If the council processes your personal data (excluding special categories of personal data) in line with one of the above bases, it does not require your consent. Otherwise, the council is required to gain your consent to process your personal data. If the council asks for your consent to process personal data, then we will explain the reason for the request. You do not need to consent or can withdraw consent later.

The council will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

Personal data gathered during the employment is held in your personnel file in hard copy and electronic format on HR and IT systems and servers. The periods for which the council holds your HR-related personal data are contained in our privacy notices to individuals.

Sometimes the council will share your personal data with contractors and agents to carry out our obligations under a contract with the individual or for our legitimate interests. We require those individuals or companies to keep your personal data confidential and secure and to protect it in accordance with Data Protection law and our policies. They are only permitted to process that data for the lawful purpose for which it has been shared and in accordance with our instructions.

The council will update HR-related personal data promptly if you advise that your information has changed or is inaccurate. You may be required to provide documentary evidence in some circumstances.

The council keeps a record of our processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

Special categories of data

The council will only process special categories of your personal data (see above) on the following basis in accordance with legislation:

- where it is necessary for carrying out rights and obligations under employment law or a collective agreement;
- where it is necessary to protect your vital interests or those of another person where you are physically or legally incapable of giving consent;
- where you have made the data public;
- where it is necessary for the establishment, exercise or defence of legal claims;
- where it is necessary for the purposes of occupational medicine or for the assessment of your working capacity;
- where it is carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates to only members or former members provided there is no disclosure to a third party without consent;
- where it is necessary for reasons for substantial public interest on the basis of law which is proportionate to the aim pursued and which contains appropriate safeguards;
- where is it necessary for reasons of public interest in the area of public health; and
- where is it necessary for archiving purposes in the public interest or scientific and historical research purposes.

If the council processes special categories of your personal data in line with one of the above bases, it does not require your consent. In other cases, the council is required to gain your consent to process your special categories of personal data. If the council asks for your consent to process a special category of personal data, then we will explain the reason for the request. You do not have to consent or can withdraw consent later.

Individual rights

As a data subject, you have a number of rights in relation to your personal data.

Subject access requests

You have the right to make a subject access request. If you make a subject access request, the council will tell you:

- whether or not your data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from yourself;
- to whom your data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long your personal data is stored (or how that period is decided);
- your rights to rectification or erasure of data, or to restrict or object to processing;
- your right to complain to the Information Commissioner if you think the council has failed to comply with your data protection rights; and
- whether or not the council carries out automated decision-making and the logic involved in any such decision-making.

The council will also provide you with a copy of your personal data undergoing processing. This will normally be in electronic form if you have made a request electronically, unless you agree otherwise.

If you want additional copies, the council may charge a fee, which will be based on the administrative cost to the council of providing the additional copies.

To make a subject access request, you should send the request to the Clerk or Chairman of the Council. In some cases, the council may need to ask for proof of identification before the request can be processed. The council will inform you if we need to verify your identity and the documents we require.

The council will normally respond to a request within a period of one month from the date it is received. Where the council processes large amounts of your data, this may not be possible within one month. The council will write to you within one month of receiving the original request to tell you if this is the case.

If a subject access request is manifestly unfounded or excessive, the council is not obliged to comply with it. Alternatively, the council can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the council has already responded. If you submit a request that is unfounded or excessive, the council will notify you that this is the case and whether or not we will respond to it.

Other rights

You have a number of other rights in relation to your personal data. You can require the council to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if your interests override the council's legitimate grounds for processing data (where the council relies on our legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not your interests override the council's legitimate grounds for processing data.
- complain to the Information Commissioner. You can do this by contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk).

To ask the council to take any of these steps, you should send the request to the Clerk or Chairman of the Council.

Data security

The council takes the security of HR-related personal data seriously. The council has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

Where the council engages third parties to process personal data on our behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Data breaches

The council have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur the council must take notes and keep evidence of that breach.

If you are aware of a data breach you must contact the Clerk or Chairman of the Council immediately and keep any evidence, you have in relation to the breach.

If the council discovers that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of yourself, we will report it to the Information Commissioner within 72 hours of discovery. The council will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, we will tell you that there has been a breach and provide you with information about its likely consequences and the mitigation measures we have taken.

International data transfers

The council will not transfer HR-related personal data to countries outside the EEA.

Individual responsibilities

You are responsible for helping the council keep your personal data up to date. You should let the council know if data provided to the council changes, for example if you move to a new house or change your bank details.

Everyone who works for, or on behalf of, the council has some responsibility for ensuring data is collected, stored and handled appropriately, in line with the council's policies.

You may have access to the personal data of other individuals and of members of the public in the course of your work with the council. Where this is the case, the council relies on you to help meet our data protection obligations to staff and members of the public. Individuals who have access to personal data are required:

- to access only data that you have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the council) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, locking computer screens when away from desk, and secure file storage and destruction including locking drawers and cabinets, not leaving documents on desk whilst unattended);
- not to remove personal data, or devices containing or that can be used to access personal data, from the council's premises without prior authorisation and without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes.
- to never transfer personal data outside the European Economic Area except in compliance with the law and with express authorisation from the Clerk or Chair of the Council
- to ask for help from the council's data protection lead if unsure about data protection or if you notice a potential breach or any areas of data protection or security that can be improved upon.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the council's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing personal data without authorisation or a legitimate reason to do so or concealing or destroying personal data as part of a subject access request, may constitute gross misconduct and could lead to dismissal without notice.

This is a non-contractual policy and procedure which will be reviewed from time to time.

Date of policy: May 2026
Approving committee: Full Council
Date of committee meeting:

Horton Parish Council's Privacy Policy

This page explains how we collect and use information

Horton Parish Council Website & Privacy Statement

Last updated: May 2026

This page informs you of our policies regarding the collection, use and disclosure of Personal Information we receive from users of the Site.

The Councils Right to Process Information
General Data Protection Regulations
We use your Personal Information only for providing and improving the Site. By using the Site, you consent and agree to the collection and use of information in accordance with this policy.

Information Collection and Use
While using our Site, we may ask you to provide us with certain personally identifiable information that can be used to contact or identify you. Personally, identifiable information may include but is not limited to your name ("Personal Information"). We may also run surveys from time-to-time, using third party websites such as Survey Monkey. We strive to anonymise the data we collect and only use it for the improvement of the services we offer.

Log Data
Like many site operators, we collect information that your browser sends whenever you visit our Site ("Log Data").
This Log Data may include information such as your computer's Internet Protocol ("IP") address, browser type, browser version, the pages of our Site that you visit, the time and date of your visit, the time spent on those pages and other statistics.
In addition, we may use third party services such as Google Analytics that collect, monitor and analyse this data. This data is completely anonymised and does not include personal information such as name or email address.

How long will we keep your data?
We hold the data securely in line with our document retention and management procedure and data map. We keep all data for as long as
a) the project it's collected for is in operation
b) on an ongoing basis but normally deleted after 10 years if our association with you is not active.

Communications
We may use your Personal Information to contact you with newsletters, should you opt into receive them.

Cookies
Cookies are files with small amount of data, which may include an anonymous unique identifier. Cookies are sent to your browser from a web site and stored on your computer's hard drive.

Like many sites, we use “cookies” to collect information. You can instruct your browser to refuse all cookies or to indicate when a cookie is being sent. However, if you do not accept cookies, you may not be able to use some portions of our Site. Please see our Cookie Statement for more information.

Security
The security of your Personal Information is important to us but remember that no method of transmission over the Internet, or method of electronic storage, is 100% secure. While we strive to use commercially acceptable means to protect your Personal Information, we cannot guarantee its absolute security.

Changes to this Privacy Policy

This Privacy Policy is effective as of May 2026 and will remain in effect except with respect to any changes in its provisions in the future, which will be in effect immediately after being posted on this page.
We reserve the right to update or change our Privacy Policy at any time and you should check this Privacy Policy periodically. Your continued use of the Service after we post any modifications to the Privacy Policy on this page will constitute your acknowledgement of the modifications and your consent to abide and be bound by the modified Privacy Policy.

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 Controller: Zannette Bougourd (Parish Clerk), 9 Redgate Park, Crewkerne. TA187NL Telephone: 07471341433, email clerk@horton-somerset-pc.gov.uk

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 our Data Controller via email: clerk@horton-somerset-pc.gov.uk to request this.

Information Deletion: If you wish Horton Parish Council to delete the information about you please contact our Data Controller via email: clerk@horton-somerset-pc.gov.uk 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 our Data Controller via email: clerk@horton-somerset-pc.gov.uk to object.

Rights Related to Automated Decision Making and Profiling Horton does not use any form of automated decision making or the profiling of individual personal data.

Conclusion: In accordance with the law, we only collect a limited amount of information about you that is necessary for correspondence, information and service provision. We do not use profiling; we do not sell or pass your data to third parties.

We do not use your data for purposes other than those specified. We make sure your data is stored securely. We delete all information deemed to be no longer necessary. We constantly review our Privacy Policies to keep it up to date in protecting your data. (You can request a copy of our policies at any time).

Complaints If you have a complaint regarding the way your personal data has been processed, you may make a complaint to Horton Parish Council Data Controller via email: clerk@horton-somerset-pc.gov.uk and the Information Commissioners Office casework@ico.org.uk Tel: 0303 123 1113

Reviewed and adopted by Horton Parish Council on: 08th May 2026

Horton Parish Council May 2026

Document Retention and Disposal Policy

1. Introduction

1.1 The Council accumulates a vast amount of information and data during the course of its everyday activities. This includes data generated internally in addition to information obtained from individuals and external organisations. This information is recorded in various different types of document.

1.2 Records created and maintained by the Council are an important asset and as such measures need to be undertaken to safeguard this information. Properly managed records provide authentic and reliable evidence of the Council's transactions and are necessary to ensure it can demonstrate accountability.

1.3 Documents may be retained in either 'hard' paper form or in electronic forms. For the purpose of this policy, 'document' and 'record' refers to both hard copy and electronic records.

1.4 It is imperative that documents are retained for an adequate period of time. If documents are destroyed prematurely the Council and individual officers concerned could face prosecution for not complying with legislation and it could cause operational difficulties, reputational damage and difficulty in defending any claim brought against the Council.

1.5 In contrast to the above the Council should not retain documents longer than is necessary. Timely disposal should be undertaken to ensure compliance with the General Data Protection Regulations so that personal information is not retained longer than necessary. This will also ensure the most efficient use of limited storage space.

2. Scope and Objectives of the Policy

2.1 The aim of this document is to provide a working framework to determine which documents are:

- Retained – and for how long; or
- Disposed of – and if so by what method.

2.2 There are some records that do not need to be kept at all or that are routinely destroyed in the course of business. This usually applies to information that is duplicated, unimportant or only of a short-term value. Unimportant records of information include:

- 'With compliments' slips.
- Catalogues and trade journals.
- Non-acceptance of invitations.
- Trivial electronic mail messages that are not related to Council business.
- Requests for information such as maps, plans or advertising material.
- Out of date distribution lists.

2.3 Duplicated and superseded material such as stationery, manuals, drafts, forms, address books and reference copies of annual reports may be destroyed.

2.4 Records should not be destroyed if the information can be used as evidence to prove that something has happened. If destroyed the disposal needs to be disposed of under the General Data Protection Regulations

3. Roles and Responsibilities for Document Retention and Disposal

3.1 Councils are responsible for determining whether to retain or dispose of documents and should undertake a review of documentation at least on an annual basis to ensure that any unnecessary documentation being held is disposed of under the General Data Protection Regulations.

3.2 Councils should ensure that all employees are aware of the retention/disposal schedule.

4. Document Retention Protocol

4.1 Councils should have in place an adequate system for documenting the activities of their service. This system should take into account the legislative and regulatory environments to which they work.

4.2 Records of each activity should be complete and accurate enough to allow employees and their successors to undertake appropriate actions in the context of their responsibilities to:

- Facilitate an audit or examination of the business by anyone so authorised.
- Protect the legal and other rights of the Council, its clients and any other persons affected by its actions.
- Verify individual consent to record, manage and record disposal of their personal data.
- Provide authenticity of the records so that the evidence derived from them is shown to be credible and authoritative.

4.3 To facilitate this the following principles should be adopted:

- Records created and maintained should be arranged in a record-keeping system that will enable quick and easy retrieval of information under the General Data Protection Regulations
- Documents that are no longer required for operational purposes but need retaining should be placed at the records office.

4.4 The retention schedules in Appendix A: List of Documents for Retention or Disposal provide guidance on the recommended minimum retention periods for specific classes of documents and records. These schedules have been compiled from recommended best practice from the Public Records Office, the Records Management Society of Great Britain and in accordance with relevant legislation.

4.5 Whenever there is a possibility of litigation, the records and information that are likely to be affected should not be amended or disposed of until the threat of litigation has been removed.

- Data is backed up regularly to an external hard drive
- Files are kept securely on a dedicated device
- Files are backed up to Adobe File Drive and iCloud drive
- Three copies of data are maintained
- Original data and two copies, stored on two distinct types of media
- At least one copy stored off site(cloud storage)

5. Document Disposal Protocol

5.1 Documents should only be disposed of if reviewed in accordance with the following:

- Is retention required to fulfil statutory or other regulatory requirements?
- Is retention required to meet the operational needs of the service?
- Is retention required to evidence events in the case of dispute?
- Is retention required because the document or record is of historic interest or intrinsic value?

5.2 When documents are scheduled for disposal the method of disposal should be appropriate to the nature and sensitivity of the documents concerned. A record of the disposal will be kept to comply with the General Data Protection Regulations.

5.3 Documents can be disposed of by any of the following methods:

- Non-confidential records: place in waste paper bin for disposal.
- Confidential records or records giving personal information: shred documents.
- Deletion of computer records.
- Transmission of records to an external body such as the County Records Office.

5.4 The following principles should be followed when disposing of records:

- All records containing personal or confidential information should be destroyed at the end of the retention period. Failure to do so could lead to the Council being prosecuted under the General Data Protection Regulations.
- the Freedom of Information Act or cause reputational damage.
- Where computer records are deleted steps should be taken to ensure that data is 'virtually impossible to retrieve' as advised by the Information Commissioner.
- Where documents are of historical interest it may be appropriate that they are transmitted to the County Records office.
- Back-up copies of documents should also be destroyed (including electronic or photographed documents unless specific provisions exist for their disposal).

5.5 Records should be maintained of appropriate disposals. These records should contain the following information:

- The name of the document destroyed.
- The date the document was destroyed.
- The method of disposal.

6. Data Protection Act 2018 – Obligation to Dispose of Certain Data

6.1 The Data Protection Act 2018 ('Fifth Principle') requires that personal information must not be retained longer than is necessary for the purpose for which it was originally obtained. Section 1 of the Data Protection Act defines personal information as:

> Data that relates to a living individual who can be identified:
> a) from the data, or
> b) from those data and other information which is in the possession of, or is likely to come into the possession of the data controller.
>
> It includes any expression of opinion about the individual and any indication of the intentions of the Council or other person in respect of the individual.

6.2 The Data Protection Act provides an exemption for information about identifiable living individuals that is held for research, statistical or historical purposes to be held indefinitely

provided that the specific requirements are met.

6.3 Councils are responsible for ensuring that they comply with the principles of the under the General Data Protection Regulations namely:

- Personal data is processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met.

- Personal data shall only be obtained for specific purposes and processed in a compatible manner.
- Personal data shall be adequate, relevant, but not excessive.
- Personal data shall be accurate and up to date.
- Personal data shall not be kept for longer than is necessary.
- Personal data shall be processed in accordance with the rights of the data subject.
- Personal data shall be kept secure.

6.4 External storage providers or archivists that are holding Council documents must also comply with the above principles of the General Data Protection Regulations.

7. Scanning of Documents

7.1 In general once a document has been scanned on to a document image system the original becomes redundant. There is no specific legislation covering the format for which local government records are retained following electronic storage, except for those prescribed by HM Revenue and Customs.

7.2 As a general rule hard copies of scanned documents should be retained for three months after scanning.

7.3 Original documents required for VAT and tax purposes should be retained for six years unless a shorter period has been agreed with HM Revenue and Customs.

8. Review of Document Retention

8.1 It is planned to review, update and where appropriate amend this document on a regular basis (at least every three years in accordance with the *Code of Practice on the Management of Records* issued by the Lord Chancellor).

8.2 This document has been compiled from various sources of recommended best practice and with reference to the following documents and publications:

- *Local Council Administration*, Charles Arnold-Baker, 12th edition, Chapter 11
- NALC LTN 40 – *Local Councils' Documents and Records*, January 2013
- NALC LTN 37 – *Freedom of Information*, July 2009
- *Lord Chancellor's Code of Practice on the Management of Records* issued under Section 46 of the *Freedom of Information Act 2000*
-

9. List of Documents

9.1 The full list of the Council's documents and the procedures for retention or disposal can be found in Appendix A: List of Documents for Retention and Disposal. This is updated regularly in accordance with any changes to legal requirements.

Appendix A: List of Documents for Retention & Disposal

List of Documents

Document	Minimum Retention Period	Reason	Disposal
Minutes & Correspondence			
Signed Minutes	Indefinite	Archive, Public inspection	N/A
Agendas	5 years	Management	RW
General emails and correspondence	Retained for as long as document is needed	Management	CW
Information from other bodies (eg CALC)	Retained for as long as document is useful	Management	RW
Local / historical information	Indefinite	To be securely kept for the benefit of the Parish	N/A
Magazines and journals	Retained for as long as document is useful	The Legal Deposit Libraries Act 2003	RW
Finance & Payroll			
Audited Accounts	Indefinite	Audit	N/A
Receipt and payment accounts	Indefinite	Archive	N/A
Receipts books of all kinds	6 years	VAT	RW
All bank statements	Last completed audit year	Audit	CW
Bank paying-in books	Last completed audit year	Audit	CW
Cheque book stubs	Last completed audit year	Audit	CW
Quotations and tenders (successful)	6 years	Limitation Act 1980 (as amended)	CW
Paid invoices	6 years	VAT	CW
Paid cheques	6 years	Limitation Act 1980 (as amended)	CW
VAT records	6 years	VAT	CW
Petty cash, postage and telephone books	6 years	Tax, VAT, Limitation Act 1980 (as amended)	CW
Timesheets	Last completed audit year 3 years	Audit Personal injury	RW
Wages / payroll	6 years from end of employment	Audit	CW
Scale of fees & charges	6 years	Management	RW
Budgets	Indefinite	Local Choice	N/A
Investments	Indefinite	Audit, Management	N/A

Human Resources			
Staff files	6 years from end of employment	Audit	CW
Job applications (unsuccessful)	6 months from time of appointment	Management	CW
Insurance			
Accident/incident reports	20 years	Potential claims	CW
Insurance policies	While valid	Management	CW
Insurance company names & policy nos	Indefinite	Management	N/A
Insurance claims	7 years after all obligations are concluded or child reaches age of 25	Limitation Act 1980 (as amended)	CW
Insurance certificates	40 years	The Employers Liability (Compulsory Insurance) Regulations 1998 (SI2753)	RW
Health & Safety inspection records	6 years	Management	RW
Miscellaneous			
Strategic Plans	Until superseded	Common Practice	RW
Policies & Operational Procedures	Until superseded	Common Practice	RW
Declarations of office	Term of office	Management	CW
Members register of interests	Term of office	Management	CW
Complaints	2 years from resolution	Management	CW
Title deeds, leases, agreements, contracts	Indefinite	Audit, Management	N/A
Members allowances register	6 years	Tax, Limitation Act 1980 (as amended)	CW
Legal/Litigation Files	6 years	Common practice	CW
Burial Grounds			
Register of: Fees collected / Burials / Purchased Graves / Plan of grave spaces / Memorials	Indefinite	Local Authorities Cemeteries Order 1977 (SI204) Management	N/A

RW – recycled waste CW – confidential waste (to be disposed of securely).

HORTON PARISH COUNCIL
IT POLICY
ADOPTED BY FULL COUNCIL FEBRUARY 2026
REVIEWED ANNUALLY.

Introduction

Each council will have its own IT setup and, as such, a single 'one-size-fits-all' IT policy is unlikely to be appropriate. Some smaller parish councils may operate with minimal equipment, while others may manage multiple devices connected to a central server. These guidelines are intended to help councils identify key considerations when developing or updating their own IT policy.

Councils that use external IT providers should ensure their policies accurately reflect current practices and contractual arrangements.

Purpose of the IT Policy

The purpose of an IT policy is to establish clear parameters for how councillors, staff, and other authorised users use council-provided technology or equipment in the course of their duties. A well-defined policy helps to:

- Set expectations for appropriate use of equipment and systems.
- Raise awareness of risks associated with IT use.
- Safeguard the council's data and digital assets.
- Clarify what constitutes acceptable and unacceptable use.
- Outline the consequences of policy breaches.

Councils will also need to determine and clearly state whether limited personal use of IT equipment is permitted (for example, checking personal email or online shopping during lunch breaks).

Monitoring of IT Use

As an IT provider, the council has the right to monitor the use of its IT equipment and systems, provided there is a legitimate reason for doing so and councillors, employees and other authorised users are informed that such monitoring may take place. Any monitoring must be proportionate and comply with relevant data protection and privacy laws. Other persons may be included if they access or use council systems e.g. if they have a council e-mail address

Scope of this policy

This policy applies to all councillors, staff, and other authorised users, regardless of their working location or pattern, including those who are home-based, office-based, or work

on a flexible or part-time basis. It sets out the expectations for the appropriate use of IT equipment and systems provided by the council.

Computer use

Hardware

1.1.1 Horton Parish Council computer equipment is provided for council purposes, however reasonable personal use is permitted (reasonable interpreted as in the opinion of the clerk). Any personal use of our computers and systems should not interrupt our daily council work in any way. Councillors, staff, and other authorised users are asked to restrict any personal use to official lunch breaks or before or after working hours.

1.1.2 All councillors, staff, and other authorised users must lock their computers when leaving their desks to prevent unauthorised access. This applies to both council-owned and personal devices used for work. Failure to comply may result in disciplinary action.

1.1.3 All computer and other electronic equipment supplied should be treated with good care at all times. Computer equipment is expensive, and any damage sustained to any equipment will have a financial impact on the council.

1.1.4 Computer and electronic hardware should be kept clean, with precautions taken to prevent food or drink spills.

1.1.5 All computer and mobile equipment will carry a number which is logged against the current owner of that equipment. A database of equipment issued will be kept.

1.1.6 Equipment should not be dismantled or reassembled without seeking advice.

1.1.7 Councillors, staff, and other authorised users are not to purchase any computer or mobile equipment (including software). Unless previously authorised.

1.1.8 Personal disks, USB sticks, CDs, DVDs, data storage devices etc cannot be used on council computers without the prior approval of the Clerk

1.1.9 All faults or necessary repairs must be reported to the Clerk

Equipment

2.1 Portable equipment

2.1.1 Portable equipment includes laptop computers, netbooks, tablets, mobile and smart phones with email capability and access to the internet etc.

2.1.2 It is particularly emphasised that council back-up procedures specific to portable equipment should be followed at all times.

2.1.3 All portable computers must be stored safely and securely when not in use in the office, i.e. when travelling or when working from home. Portable equipment (unless locked in a secure cabinet or office) should be kept with or near the user at all times; should not be left unattended when away from council premises and should never be left in parked vehicles or at any council or non-council premises.

2.1.4 It is important to ensure all portable devices are protected with encryption in case they are lost or stolen. All smartphones or tablets that hold council data, including emails and files, must be protected with a pin code. Where possible, these devices should also be programmed to erase all content after several unsuccessful attempts to break in. Any security set on these devices must not be disenabled or removed.

2.1.5 Multi-Factor Authentication (MFA) is a security process that requires users to verify their identity using two or more independent methods—for example, entering a password (something you know) and confirming a code sent to your mobile device (something you have). This significantly reduces the risk of unauthorised access to systems and sensitive data. NALC recommends implementing MFA as a best practice to enhance information security and support compliance with data protection obligations under the UK GDPR and the Data Protection Act 2018.

2.1.6 If an item of portable equipment is lost or damaged this should be reported to the Clerk.

2.1.7 To protect confidential information, unless it is a requirement of the job and this has been authorised, it is forbidden for photographs or videos to be taken on council premises, without the prior written permission of the Clerk. This includes mobile

telephones with camera function, camcorder, tape or other recording device for sound or pictures - moving or still.

2.1.8 Under no circumstances should any non-public meeting or conversation be recorded without the permission of those present. This does not affect statutory rights (under The Openness of Local Government Regulations 2014).

2.1.9 In addition, the council does not permit webcams (which may be pre-installed on many laptops) to be used in the workplace, other than for conference calls for council purposes. If there is any doubt as to whether a device falls under this clause, advice should be sought from the Clerk.

2.2 Use of own devices

2.2.1 Personal laptops and other computers or other devices should not be brought into work and used to access council IT systems during working hours, unless this has been authorised by their line manager. This is to ensure that no viruses enter the system, to prevent time being wasted during working hours on personal use and to assist in maintaining security, confidentiality, and data protection.

2.2.2 The council recognises that some councillors, staff, and other authorised users may wish to use their own smartphones, tablets, laptops etc to access our servers, private clouds or networks for normal council purposes, including, but not limited to, reading their emails, accessing documents stored on the council's website or to store data on the council's server(s) or access data in other services. Any such use of personal devices will be at the discretion of the council, but consent for standard systems (MS Windows) will normally be permitted. Such devices should be kept up to date so that any vulnerabilities in the operating system or other software on the device are appropriately patched or updated.

2.2.3 However, the same security precautions apply to personal devices as to the council's desktop equipment. For continuity purposes, calls made to external parties must be made on council landlines or mobile phone numbers to ensure that only these numbers are used and/or stored by the recipient, rather than personal numbers. Any emails sent from own devices should be sent from a council email account and should not identify the individual's personal email address.

2.2.4 Councillors, staff, and other authorised users that use council systems are expected to use all devices in an ethical and respectful manner and in accordance with this policy. Accessing inappropriate websites or services on any device via the IT infrastructure that is paid for or provided by the council carries a high degree of risk, and, for employees, may result in disciplinary action, including summary dismissal (without notice). For Workers or Contractors, we may terminate the worker agreement. This is irrespective of the ownership of the device used. An example would be downloading copyright music illegally or accessing pornographic material.

2.2.5 In cases of legal proceedings against the council, the council may need to temporarily take possession of a device, whether council-owned or personal to retrieve the relevant data.

2.2.6 Wherever possible the user should maintain a clear separation between the personal data processed on the council's behalf and that processed for their own personal use, for example, by using different apps for council and personal use. If the device supports both work and personal profiles, the work profile must always be used for work-related purposes.

2.2.7 Councillors, staff, and other authorised users who intend to use their own devices via the council's infrastructure must ensure that they:

- use a strong password or fingerprint to protect their device(s) from being accessed. For smartphones and tablets this should lock the device after three failed login attempts.
- configure their device(s) to automatically prompt for a password after a period of inactivity of more than 10 minutes
- always password protect any documents containing confidential information that are sent as attachments to an email, and notify the password separately (preferably by a means other than email).
- for smartphones and tablets, activate the automatic device wipe function (where available). Note that use of the remote wipe function may also involve the removal of the individual's personal data. Councillors, staff, and other authorised users are therefore advised to keep personal data separate from council data and where possible ensure secure Wi-Fi networks are used.

- ensure that work-related data cannot be viewed or retrieved by family or friends who may use the device.
- inform the Clerk if their device(s) is/are lost, stolen, or inappropriately accessed where there is risk of access to council data or resources. To prevent phones being used, they will need to retain the details of their IMEI number and the SIM number of the device as their provider will require this to deactivate it.

2.2.8 Personal data relating to councillors, staff, and other authorised users, residents, and external stakeholders should not be saved to any personal accounts with third-party storage cloud service providers as this may breach data protection legislation or create a security risk if the device is lost or stolen. This applies especially if the passwords used to store/access data are saved onto the device, or if the service permits councillors, staff, and other authorised users to remain logged in between sessions.

2.2.9 Personal information and sensitive data should never be saved on councillors, staff, or other authorised users own devices as this may breach confidentiality agreements, especially if the device is used by other people from time to time. The following data must never be accessed or processed on a personal device :

- Personal contact details (names, addresses, telephone numbers, email addresses)
- Financial information (bank details, payment card information, payroll data)
- Health or medical records
- Sensitive personal data (relating to race, ethnicity, religion, sexual orientation)
- Criminal records or allegations
- Safeguarding information concerning children or vulnerable adults
- Commercially sensitive information (contracts, tenders, procurement details)
- Staff personnel files and disciplinary records
- Legal advice and correspondence
- Passwords, access credentials, or security information

Personal devices * include personal laptops, desktop computers, mobile phones, smartphones, tablets, iPads, USB drives, external hard drives, smartwatches, wearable devices, and home computers shared with family members.

2.2.10 If removable media are used to transfer data (e.g. USB drives or CDs), the user must also securely delete the data on the media once the transfer is complete.

2.2.11 Councillors, staff, and other authorised users who open any attachments should ensure that any cached copies are deleted immediately after use. The Clerk will provide assistance or training in doing this if needed. Additional risks include data belonging to the council being accessed by unauthorised persons if the device(s) is lost, stolen, or used without the owner's permission.

2.2.12 Any work done on user's own equipment should be stored securely and password protected and should always be backed up in accordance with the council's standard backup procedures.

2.2.13 If transferring data, either by email or by other means, this should be done through an encrypted channel, such as a virtual private network (VPN) or a secure web protocol (https://). Unsecured wireless networks should not be used.

2.2.14 Prior to the disposal of any device that has work data stored on it, and in the event of a user leaving the council, councillors, staff, and other authorised users are required to allow the Clerk or IT services provider access to the device to ensure that all passwords, user access shortcuts and any identifiable data are removed from the device.

2.2.15 Councillors, staff, and other authorised users must take responsibility for understanding how their device(s) work in respect to the above rules if they are accessing council servers/services via their own IT equipment. Risks to the user's personal device(s) include data loss as a result of a crash of the operating system, bugs and viruses, software or hardware failures and programming errors rendering a device inoperable. The council will use reasonable endeavours to assist, but councillors, staff, and other authorised users are personally liable for their own device(s) and for any costs incurred as a result of the above.

Health and safety

3.1.1 Councillors, staff, and other authorised users who work in council offices will be provided with an appropriate workstation.

3.1.2 The Council has a duty to ensure that regular appropriate eye tests, carried out by a competent person, are offered to employees using display screen equipment. Further details are set out in the council's health and safety policy.

3.1.3 Any VDU user who feels that their workstation requires changes to make it compliant must speak to the Clerk.

If any hazards are detected at a workstation, including 'noises' from the IT equipment, this should be reported immediately to the Clerk.

Password and Authentication Policy

4.1.1 All user accounts must be protected by strong, secure passwords. The council follows the National Cyber Security Centre (NCSC) recommendations for creating passwords using three random words (e.g. PurpleCandleRiver). This method helps create passwords that are both strong and easy to remember, while offering effective protection against common cyber threats such as brute-force attacks. This approach is endorsed in NALC guidance.

In addition to strong passwords, Multi-Factor Authentication (MFA) should be enabled wherever possible. MFA requires users to provide two or more independent forms of verification—for example, a password (something you know) and a code sent to your phone (something you have). This significantly reduces the risk of unauthorised access to systems and personal data.

To further strengthen account security:

- Initial user account passwords must be generated by the IT provider.
- Default passwords provided by vendors or the IT provider must be changed immediately upon installation or setup.
- Service or System (e.g. Website) account passwords are generated and managed by the IT provider.
- The council recommends these practices as part of its commitment to robust information security and to support compliance with the UK GDPR and the Data Protection Act 2018.

For more guidance, see the NCSC's advice on password security: NCSC Password Guidance

4.1.2 Access to Passwords

- Passwords are personal and must not be shared under any circumstances.

- Only the assigned user of an account may access or use the associated password.
- In exceptional cases (e.g., incident response or employee offboarding), access to system credentials may be granted to authorised personnel from the IT provider with appropriate approvals and logging.
- Administrative credentials must be stored securely and only accessible to authorised personnel with a copy provided to the chair of council], in a sealed envelope, only to be accessed in an emergency.

4.1.3 Password Storage and Management

- Passwords must not be stored in plain text or written down in insecure locations.
- Passwords must be stored using a council-approved, encrypted password manager (e.g., LastPass, Bitwarden, or KeePass).

4.1.4 Password Change Requirements

- Immediately change password if compromise is suspected.

4.1.5 Password Access Control and Logging

- All access to administrative or shared credentials must be logged and auditable.
- Attempts to access unauthorized passwords will be treated as a security incident.

4.1.6 Responsibility

- Users are responsible for creating and maintaining secure passwords for their accounts.

4.1.7 The IT security provider is responsible for:

- Managing system/service credentials.
- Enforcing password policies. Auditing and monitoring password-related security practices.

Monitoring

5.1.1 The council reserves the right to monitor and maintain logs of computer usage and inspect any files stored on its network, servers, computers, or associated technology to ensure compliance with this policy as well as relevant legislation. Internet, email, and computer usage is continually monitored as part of the council's protection against computer viruses, ongoing maintenance of the system, and when investigating faults.

5.1.5 The council will monitor the use of electronic communications and use of the internet in line with the Investigatory Powers (Interception by Councils etc for Monitoring and Record-keeping Purposes) Regulations 2018.

5.1.6 Monitoring of an employee's or user's email or and/or internet use will be conducted in accordance with an impact assessment that the council has carried out to ensure that monitoring is necessary and proportionate. Monitoring is in the council's legitimate interests and is to ensure that this policy is being complied with.

5.1.7 The information obtained through monitoring may be shared internally, including with relevant councillors and IT staff if access to the data is necessary for performance of their roles. The information may also be shared with external HR or legal advisers for the purposes of seeking professional advice. Any external advisers will have appropriate data protection policies and protocols in place.

5.1.8 The information gathered through monitoring will be retained only long enough for any breach of this policy to come to light and for any investigation to be conducted.

5.1.9 Councillors, staff, and other authorised users have a number of rights in relation to their data, including the right to make a subject access request and the right to have data rectified or erased in some circumstances. You can find further details of these rights and how to exercise them in the council's data protection policy.

5.1.10 Such monitoring and the retrieval of the content of any messages may be for the purposes of checking whether the use of the system is legitimate, to find lost messages or to retrieve messages lost due to computer failure, to assist in the investigation of wrongful acts, or to comply with any legal obligation.

5.1.11 The council has software and systems in place that can monitor and record all internet usage.

5.1.12 The council reserves the right to inspect all files stored on its computer systems in order to assure compliance with this policy. The council also reserves the right

to monitor the types of sites being accessed and the extent and frequency of use of the internet at any time, both inside and outside of working hours to ensure that the system is not being abused and to protect the council from potential damage or disrepute.

5.1.13 Any use that the council considers to be 'improper', either in terms of the content or the amount of time spent on this, may result in disciplinary proceedings.

5.1.14 All computers will be periodically checked and scanned for unauthorised programmes and viruses.

Remote working

6.1.1 Increased IT security measures apply to those who work away from their normal place of work (e.g. whilst travelling, working from home or any other different venue as follows:

- if logging into the council's systems or services remotely, using computers that either do not belong to the council or are not owned by the user, any passwords must not be saved, and the user must log out at the end of the session deleting all logs and history records within the browser used. If the configuration of the device does not clearly support these actions (for example at an internet café), council services should not be accessed from that device.
- the location and direction of the screen should be checked to ensure confidential information is out of view. Steps should be taken to avoid messages being read by other people, including other travellers on public transport etc.
- any data printed should be collected and stored securely.
- all electronic files should be password protected and the data saved to the council's system/services when accessible.
- papers, files or computer equipment must not be left unattended at "non council" premises unless arrangements have been made with a responsible person at a "noncouncil" premises for them to be kept in a locked room or cabinet if they are to be left unattended at any time.
- any data should be kept safely and should only be disposed of securely.
- papers, files, data sticks/storage, flash drive or backup hard drives should not be left unattended in cars, except where it is entirely unavoidable for short periods, in which case they must be locked in the boot of the car. If staying away overnight,

council data should be taken into the accommodation, care being taken that it will not be interfered with by others or inadvertently destroyed.

- where possible the ability to remotely wipe any mobile devices that process sensitive information should be retained in the case of loss or theft.
- Councillors, staff, and other authorised users who work away from the office with sensitive data should be equipped with a screen privacy filter for mobile devices and should use this at all times when accessing such data away from the office.

Email

7.1.1 Council email facilities are intended to promote effective and speedy communication on work-related matters. Although we encourage the use of email, it can be risky. Councillors, staff, and other authorised users need to be careful not to introduce viruses onto council systems and should take proper account of the security advice below.

7.1.2 On occasion, it will be quicker to action an issue by telephone or face to face, rather than via protracted email chains. Emails should not be used as a substitute for face to face or telephone conversations. Councillors, staff, and other authorised users are expected to decide which is the optimum channel of communication to complete their tasks quickly and effectively.

7.1.3 These rules are designed to minimise the legal risks run when using email at work and to guide councillors, staff, and other authorised users as to what may and may not be done. If there is something which is not covered in the policy, councillors, staff, and other authorised users should ask the Clerk rather than assuming they know the right answer.

7.1.4 All councillors, staff, and other authorised users who need to use email as part of their role will normally be given their own council email address and account. The council may, at any time, withdraw email access, should it feel that this is no longer necessary for the role or that the system is being abused.

7.1.5 Email messages sent on the council's account are for council use only. Personal use is not permitted.

Use of the Internet

8.1 Copyright

8.1.1 Much of what appears on the Internet is protected by copyright. Any copying without permission, including electronic copying, is illegal and therefore prohibited. The Copyright, Designs and Patents Act 1988 set out the rules. The copyright laws not only apply to documents but also to software.

The infringement of the copyright of another person or organisation could lead to legal action being taken against the council and damages being awarded, as well as disciplinary action, including dismissal, being taken against the perpetrator.

8.1.2 It is easy to copy electronically, but this does not make it any less an offence. The council's policy is to comply with copyright laws, and not to bend the rules in any way.

8.1.3 Councillors, staff, and other authorised users should not assume that because a document or file is on the Internet, it can be freely copied. There is a difference between information in the 'public domain' (which is no longer confidential or secret information but is still copyright protected) and information which is not protected by copyright (such as where the author has been dead for more than 70 years).

8.1.4 Usually, a website will contain copyright conditions; these warnings should be read before downloading or copying.

8.1.5 Copyright and database right law can be complicated. Councillors, staff, and other authorised users should check with the Clerk if unsure about anything.

8.2 Trademarks, links and data protection

8.2.1 The council does not permit the registration of any new domain names or trademarks relating to the council's names or products anywhere in the world, unless authorised to do so. Nor should they add links from any of the council's web pages to any other external sites without checking first with the Clerk.

8.2.2 Special rules apply to the processing of personal and sensitive personal data. For further guidance on this, see the council's data protection policy.

8.3 Accuracy of information

8.3.1 One of the main benefits of the internet is the access it gives to large amounts of information, which is often more up to date than traditional sources such as libraries. Be aware that, as the internet is uncontrolled, much of the information may be less accurate than it appears.

Use of social media

9.1.1 Social media includes blogs; Wikipedia and other similar sites where text can be posted; multimedia or user generated media sites (YouTube); social networking sites (such as Facebook, LinkedIn, X (formerly known as Twitter), Instagram, TikTok, etc.); virtual worlds (Second Life); text messaging and mobile device communications and more traditional forms of media such as TV and newspapers. Care should be taken when using social media at any time, either using council systems or at home.

9.1.2 Personal use of social networking/media and chat sites are not permitted during working hours.

9.1.3 The council recognises the importance of councillors, staff, and other authorised users joining in and helping to shape sector conversation and enhancing its image through blogging and interaction in social media. Therefore, where it is relevant to use social networking sites as part of the individual's position, this is acceptable.

However, inappropriate comments and postings can adversely affect the reputation of the council, even if it is not directly referenced. If comments or photographs could reasonably be interpreted as being associated with the council, or if remarks about the council could be regarded as abusive, humiliating, sexual harassment, discriminatory or derogatory, or could constitute bullying or harassment, the council will treat this as a serious disciplinary offence. Councillors, staff, and other authorised users should be aware that parishioners or other local organisations may read councillors, staff, and other authorised users' personal weblogs, to acquire information, for example, about their work, internal council business, and employee morale. Therefore, even if the council is not named, care should be taken with any views expressed.

9.1.4 To protect both the council and its interests, everyone is required to comply with the following rules about social media, whether in relation to their council role or personal social networking sites, and irrespective of whether this is during or after working hours:

9.1.5

- Contacts from any of the council's databases should not be downloaded and connected with on LinkedIn or other social networking sites with electronic address book facilities, unless this has been authorised.
- Any blog that mentions the council, its current work, councillors, employees, other users associated with the council, partner organisations, local groups, suppliers, parishioners, should identify the author as one of its councillors or employees and state that the views expressed on the blog or website are theirs alone and do not represent the views of the Council. Even if the council is not mentioned, care should be taken with any views expressed on social media sites and any views should clearly be stated to be the writer's own (e.g. via a disclaimer statement such as: "The comments and other content on this site are my own and do not represent the positions or opinions of my employer/ the council.") Writers must not claim or give the impression that they are speaking on behalf of the council.
- The Council expects councillors, staff, and other authorised users to be respectful about the council and not to engage in any name calling or any behaviour that will reflect negatively on its reputation. Any unauthorised use of copyright materials, any unfounded or derogatory statements, or any misrepresentation is not viewed favourably and could constitute gross misconduct.
- Photos or videos that include employees or other workers wearing uniforms or clothing displaying the council's name or logo should not be posted on social media if they could reflect negatively on the individual, their role, their colleagues, or the council. Additionally, photos, videos, or audio recordings must not be taken on council premises without explicit permission
- Comments posted by councillors, staff, and other authorised users on any sites should be knowledgeable, accurate and professional and should not compromise the council in any way.
- Inappropriate conversations with [residents and external stakeholders"] should not take place on any social networking sites, including forums.
- Any writing about or displaying photos or videos of internal activities that involves current councillors, staff, and other authorised persons, might be considered a breach of data protection and a breach of privacy and confidentiality. Therefore, their permission should be gained prior to uploading any such material. Details of any kind relating to any events, conversations, materials or documents that are meant to be private, confidential or internal to the council should not be posted. This may include manuals; procedures; training documents; non-public financial or operational information; personal information regarding other councillors, staff, and other authorised users anything to do with a disciplinary case, grievance, allegation of

bullying/harassment or discrimination, or legal issue; any other secret, confidential, or proprietary information or information that is subject to confidentiality agreements. This does not affect statutory requirements to publish information including under the Freedom of Information Act.

- Councillors, staff, and other authorised users must be aware that they are personally liable for anything that they write or present online (including on an online forum or blog, post, feed or website). Councillors should always be mindful of the Members Code of Conduct and Nolan Principles. Employees may be subject to disciplinary action for comments, content, or images that are defamatory, embarrassing, pornographic, proprietary, harassing, libellous, or that can create a hostile work environment. They may also be sued by other organisations, and any individual or council that views their comments, content, or images as defamatory, pornographic, proprietary, harassing, libellous or creating a hostile work environment. In addition, other councillors, staff, and other authorised users can raise grievances for alleged bullying and/or harassment.
- Postings to websites or anywhere on the internet and social media of any kind, or in any press or media of any kind, should not breach copyright or other law or disclose confidential information, defame or make derogatory comments about the council or staff, or disclose personal data or information about any individual that could breach data protection legislation.
- Contacts by the media relating to the council, should be referred to the Clerk or Communications Officer.
- Councillors, staff, and other authorised users who use sites such as LinkedIn and Facebook must ensure that the information on their profile is accurate and up to date and must update their profile on leaving the council.
- Councillors, staff, and other authorised users who use X.com, LinkedIn, or other social media/networking sites for council development purposes must ensure they provide the council with login details, including password(s), so that these sites can be accessed and updated in their absence.
- Councillors, staff, and other authorised users who have left the council must not post any inappropriate comments about the council or its councillors, staff, and other authorised users on LinkedIn, Facebook, X.com or any other social media/networking sites.
- During your employment/ involvement with the council, you may create or obtain access to a variety of professional contacts and confidential information. This includes, but is not limited to, contacts made through professional networking platforms such as LinkedIn, where those contacts have been established or maintained in your capacity as a councillor, member of staff, or

another authorised user. All such contacts will be considered council property and may be subject to disclosure upon request.

9.1.6 Note that the council may, from time to time, monitor external postings on social media sites. Any employee who has a profile (for example on LinkedIn or Facebook) must not misrepresent themselves or their role with the council. Councillors, staff, and other authorised users are also advised that social media sites are not an appropriate place to air council concerns or complaints: these should be raised with the council or formally through the grievance procedure.

9.1.7 It is important to note that resident and external stakeholder contact details and information remain the property of the council. In addition, councillors, staff, and other authorised users leaving the council will be required to delete all council-related data including resident and external stakeholders contact details from any personal device/equipment.

Misuse

Misuse of IT systems and equipment is not in line with the council's standards of conduct and will be taken seriously. Any inappropriate or unauthorised use may lead to formal action, including disciplinary proceedings or, in serious cases, dismissal.

Guidance

Where there is text in [square brackets] this part may be updated or be deleted if not relevant. An alternative option may have been provided.

Important notice

Horton Parish Council Email Deletion and Retention Policy

1. Purpose
This policy sets out how the Parish Council manages, retains, and deletes emails in line with its obligations under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and relevant local government records management guidance.

---

2. Scope
This policy applies to all email communications sent or received through official Parish Council email accounts. The retention periods are different to any general Data Retention Policy as the regulations surrounding digital communications are more stringent.

---

3. Policy Principles

- Emails are considered a form of official record and must be managed accordingly.
- Personal data contained in emails must be handled securely and only retained as long as necessary.
- Emails should not be used for long-term storage of information - relevant data, such as quotes and and disciplinary or legal matters, should be transferred to formal record-keeping systems, which will be managed by the Clerk.

---

4. Email Retention Periods

- It is not practical to expect unpaid Councillors to individually assess emails and have different retention periods for different categories of emails, so a single period is to be used.
- This period is to be set at three years after the end of the current financial year.
- Emails containing information or documents required for longer-term retention must be exported and passed to the Clerk for archiving once the email deletion period is reached. This includes, but is not limited to, contractual and legal matters, and these archived documents are to be kept according to the Councils document retention policy.
- Emails must be deleted after the relevant retention period has elapsed.

---

5. Security and Access

- The PC email system is to be managed by the Clerk, or any appointed third parties, such as technical or legal support professionals.
- For the avoidance of doubt, this does not include any existing Parish Councillors, who are not permitted to not have access to any email account except their own.
- Only authorised individuals should access Parish Council email accounts. Proper digital security must be maintained on any devices where digital communications are stored
- When an individual leaves their role, their email account must be archived until the relevant deletion period has expired, when it may be deleted by the Clerk.
- If the Clerk or the Chair change, then their official email accounts must be archived and the accounts passed over without any messages present. People emailing either of these two official accounts do so in the expectation of privacy, and that these messages will not be read

by any third parties without authorisation, even if the job role changes.

- No access may be made to any current or archived account by the Clerk except by direct authorisation of the Parish Council and then only for legal or contractual reasons or to comply with any Freedom of Information Act (FOI), Subject Access Request.

---

6. Email Backup
Email systems may be backed up for disaster recovery purposes; however, backup copies are not used for routine access and will be retained no longer than necessary for technical purposes.

---

7. Responsibilities

- The Parish Clerk is responsible for overseeing compliance with this policy.
- All councillors and staff must adhere to this policy. Failure to do this is a disciplinary offence.

---

8. Review and Updates
This policy will be reviewed every 3 years or sooner if there is a significant change in legislation or Council operations.

Horton Parish Council Data Breach Policy - 2026

1 Purpose
This policy sets out how the Parish Council identifies, manages, reports, and learns from personal data breaches. It ensures compliance with:
UK GDPR
Data Protection Act 2018
ICO guidance on personal data breaches
The aim is to minimise harm to individuals, protect the Council's information assets, and maintain public trust.

2 Scope
This policy applies to:
All personal data processed by the Parish Council
All councillors, employees, volunteers, and contractors
All formats (paper, electronic, email, audio, images, website, social media, CCTV)
It covers accidental and deliberate breaches.

3 What is a Personal Data Breach?
A personal data breach is any incident that leads to:
Unauthorised access
Unauthorised disclosure
• Loss or theft
Destruction or alteration
Loss of availability
Examples include:
Sending personal data to the wrong recipient
Losing an unencrypted laptop or USB stick
Emailing documents to a personal account
Accidental deletion of key records
Website exposure of personal information
Ransomware or cyber-attack

4 Roles & Responsibilities
The Parish Council
Holds overall responsibility for compliance
Receives reports on breaches and approves corrective actions
Clerk / Responsible Officer
Acts as the Data Breach Manager
Leads breach investigation and documentation
Assesses risk and determines whether the ICO must be notified
Ensures affected individuals are informed where required
Maintains the Breach Register
Councillors, Staff, and Volunteers
Must report all suspected breaches immediately
Must not attempt to hide or resolve breaches informally
Must cooperate with investigations

5 Identifying a Breach
Any person who becomes aware of a possible breach must report it immediately to the Clerk. Delays increase risk and may breach the Council's legal duty to notify the ICO within 72 hours.
Indicators of a breach include:
Unexpected system behaviour
Missing files or unexplained deletions
Complaints from individuals
Suspicious emails or phishing attempts
Lost or stolen devices

6 Reporting a Breach
All suspected breaches must be reported using the Council's Data Breach Report Form.
Reports must include:
What happened
When and how it was discovered
What data is involved
Who is affected
Any immediate actions taken

7 Containment and Recovery
The Clerk will take immediate steps to limit the impact, which may include:
Isolating affected systems
Resetting passwords
Recovering deleted data from backups
Contacting IT support
Securing physical records
Requesting return or deletion of mis-sent information

8 Assessing the Risk
The Clerk will assess:
The type and sensitivity of the data
The number of individuals affected
The potential harm (identity theft, distress, financial loss, reputational damage)
Whether the data was encrypted or protected
Whether the breach is likely to result in a risk to individuals' rights and freedoms
This assessment determines whether the ICO and affected individuals must be notified.

9 Notification Requirements
9.1 Notifying the ICO
The Council must notify the ICO within 72 hours if the breach is likely to result in a risk to individuals.
The notification will include:
Nature of the breach
Categories and volume of data affected
Likely consequences
Measures taken or proposed
Contact details for the Clerk
If the Council decides not to notify the ICO, the reasoning must be documented.

9.2 Notifying Individuals
Individuals must be informed without undue delay if the breach is likely to result in a high risk to their rights and freedoms.
Notifications must:
Describe the breach in clear language
Explain potential impacts
Provide advice on protective steps
Give contact details for support

10 Documentation
The Clerk will maintain a Data Breach Register containing:
Description of the breach
Date discovered
Risk assessment
Decisions on notification
Actions taken
Lessons learned
This register must be retained in line with the Council's retention schedule.

11 Learning and Prevention
After each breach, the Council will:
Review what went wrong
Update policies or procedures
Provide additional training if needed
Improve technical or organisational controls
Patterns of repeated breaches will trigger a formal review.

12 Training and Awareness
All councillors, staff.

13. Approval
This policy was adopted by the Parish Council at its meeting on: 18/05/2026

Signed: Chair of the Council Clerk / Responsible Officer

Horton Parish Council

Data Security Breach Reporting Form
In the case of a breach or potential breach to be submitted to clerk@horton-somerset-pc.gov.uk

A data security breach can happen for a number of reasons: Loss or theft of data or equipment on which data is Stored; Inappropriate access controls allowing unauthorised use; Equipment failure; Human error; Unforeseen circumstances such as a fire or flood; Hacking attack; 'Blagging' offences where information is obtained by deceiving the organisation who holds it. Use this form to report such breaches.

Example: Reportable Theft or loss of an unencrypted laptop computer or other unencrypted portable electronic/digital media holding names, addresses, dates of birth and National Insurance Numbers of individuals. A manual paper-based filing system (or unencrypted digital media) holding the personal data relating to named individuals and their financial records etc. More information can be found using the below link:

https://ico.org.uk/media/for-organisations/documents/1562/guidance_on_data_security_breach_management.pdf

Breach Containment and Recovery

Article 2(2) of the Notification Regulation states:

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

Date and time of Notification of Breach	
Notification of Breach to whom Name Contact Details	

Details of Breach	
Nature and content of Data Involved	
Number of individuals affected:	
Name of person investigating breach Name Job Title Contact details Email Phone number Address	
Information Commissioner informed Time and method of contact https://report.ico.org.uk/security-breach/	
Police Informed if relevant Time and method of contact Name of person contacted Contact details	
Individuals contacted How many individuals contacted? Method of contact used to contact? Does the breach affect individuals in other EU member states? What are the potential consequences and adverse effects on those individuals?	

Confirm that details of the nature of the risk to the individuals affected: any measures they can take to safeguard against it; and the likely cost to them of taking those measures is relayed to the individuals involved.	
Staff briefed	
Assessment of ongoing risk	
Containment Actions: technical and organisational security measures have you applied (or were to be applied) to the affected personal data	
Recovery Plan	
Evaluation and response	

Adopted May 2026

Review May 2027

HORTON PARISH COUNCIL

9 Redgate Park, Crewkerne. TA18 7NL

clerk@horton-somerset-pc.gov.uk

HORTON PARISH COUNCIL FREEDOM OF INFORMATION POLICY

Adopted May 2026

The Parish Council is committed to openness and transparency and wishes to make relevant information available wherever possible to individuals who may request it, subject to safeguarding the privacy of individuals and to legitimate considerations of national security, law enforcement and commercial interests where relevant. The Freedom of Information Act gives everyone a statutory right of access to information held by bodies such as the Parish Council.

Model publication scheme

This document is based on the revised model publication scheme issued by the Information Commissioner's Office. The model scheme is at www.ico.org.uk/model-publication-scheme.pdf

Information about the Parish Council

A significant amount of information about the Parish Council is available on its website. The Parish Council Clerk should be contacted if information is needed in an alternative format.

Making a request for information

Individuals or organisations may make a written request for other information which they believe the Parish Council holds. To request information under the provisions of the Act an email (or if not possible: a letter) should be sent to the Clerk at clerk@horton-somerset-pc.gov.uk or by letter to the Clerk's address. This should include the full name and valid postal address of the person or organization making the request, as required under the Act, and a clear description of the information sought.

When a request is made, a preference about the desired format of the information may be made: for example: hard copy, an opportunity to inspect a record containing the information, or providing a digest or summary of the information. The Council will try to meet the preference as far as is reasonably practical or explain if it cannot do so.

It is noted that when forwarding on documents and especially emails in a digital format, that mistakes over GDPR regulations can easily be made. Names and contact information that should remain private can easily be sent out to third parties. It is further noted that it is impossible to redact forwarded emails, and that documents can include metadata, the disclosure of which can be contrary to GDPR regulations. It is also acknowledged that Horton Parish Council has inadvertent disclosed such information in the past, and consequently, and to avoid these mistakes being made, the Parish Council deems that it is reasonable to have a policy to only send out hard copies of any documents, and that before these documents are sent to the Requestor, they will be checked by a Councillor and any personal information redacted. Each page will be initialled by said councillor to indicate that it has been checked. To ensure that there is an adequate accountability and paper trail, the redacted documents will be sent Special Delivery.

Responding to requests

The Council will inform the person or organisation making the request in writing whether it holds the information requested and if so, provide it to not later than 20 working days after it receives the request. The Freedom of Information Act identifies several categories of information which the Parish Council is not

required to disclose under the Act. In this case, the Council will write stating the exemption which provides the basis for refusal within the Act and why it applies to the information requested. The Council will communicate this within the above 20-day time period.

Charges for providing information under the Freedom of Information Act
There is no 'flat rate' fee to receive information and in many cases the Council will provide the information free of charge. However, it should be noted that if the information sought is not readily available in the form in which it is requested, the Parish Council may charge a fee based on the costs associated with providing the information, for example photocopying and postage (known as 'disbursements'). The Freedom of Information Act does permit the Parish Council to refuse a request if it estimates that it will cost in excess of the appropriate cost limit (currently £450) to fulfil that request.

Freedom of information Fees Notice
If it is necessary to charge a fee for disbursements, or because the costs exceed the appropriate limit, the Council will write advising of the fee required within 20 working days of receipt of the request. This is known as a 'Fees Notice'. When a Fees Notice is issued, the noted 20-day limit for a response will stop, and will start again when the Council receives payment. If the fee is not received within three months the Council is not obliged to comply with the request.

The current printing and scanning costs are as follows:

A4 black and white print out: 17 pence per page

A4 colour print out: 60 pence per page

A4 scan: 50 pence per page

Transparency of requests

Horton Parish Council is committed to a policy of transparency, and so will publish as much information about each request as it is legally allowed to. They will also publish information that allows parishioners to see the costs of every request, and information that will allow parishioners to see if multiple requests are being made, in order to allow Parishioners to check that the Parish Council are doing enough to tackle repeat and vexatious requests.

Transparency notwithstanding, Horton Parish Council will not publish any information that is contrary to the prevailing GDPR regulations.

Costs of requests
It is noted that any time that it takes to gather the information for any request may fall outside of the usual paid hours of any Council Officer or employee and in this case these hours will be payable at their usual hourly rate or the statutory rate of £25 per hour whichever is higher, and that this will be payable even if the total chargeable falls below the Fees Notice threshold.

Complaints
If anyone is dissatisfied with the way the Parish Council has responded to a request for information, they should write to:

Horton Parish Council, 9 Redgate Park, Crewkerne. TA187NL clerk@horton-somerset-pc.gov.uk

Model publication scheme

Freedom of Information Act

This model publication scheme has been prepared and approved by the Information Commissioner. It may be adopted without modification by any public authority without further approval and will be valid until further notice.

This publication scheme commits an authority to make information available to the public as part of its normal business activities. The information covered is included in the classes of information mentioned below, where this information is held by the authority. Additional assistance is provided to the definition of these classes in sector specific guidance manuals issued by the Information Commissioner.

The scheme commits an authority:

- To proactively publish or otherwise make available as a matter of routine, information, including environmental information, which is held by the authority and falls within the classifications below.
- To specify the information which is held by the authority and falls within the classifications below.
- To proactively publish or otherwise make available as a matter of routine, information in line with the statements contained within this scheme.
- To produce and publish the methods by which the specific information is made routinely available so that it can be easily identified and accessed by members of the public.
- To review and update on a regular basis the information the authority makes available under this scheme.
- To produce a schedule of any fees charged for access to information which is made proactively available.
- To make this publication scheme available to the public.
- To publish any dataset held by the authority that has been requested, and any updated versions it holds, unless the authority is satisfied that it is not appropriate to do so; to publish the dataset, where reasonably practicable, in an electronic form that is capable of re-use; and, if any information in the dataset is a relevant copyright work and the public authority is the only owner, to make the information available for re-use under the terms of the Re-use of Public Sector Information Regulations

2015, if they apply, and otherwise under the terms of the Freedom of Information Act section 19.
The term 'dataset' is defined in section 11(5) of the Freedom of Information Act. The term 'relevant copyright work' is defined in section 19(8) of that Act.

Classes of information

Who we are and what we do.
Organisational information, locations and contacts, constitutional and legal governance.

What we spend and how we spend it.
Financial information relating to projected and actual income and expenditure, tendering, procurement and contracts.

What our priorities are and how we are doing.
Strategy and performance information, plans, assessments, inspections and reviews.

How we make decisions.
Policy proposals and decisions. Decision making processes, internal criteria and procedures, consultations.

Our policies and procedures.
Current written protocols for delivering our functions and responsibilities.

Lists and registers.
Information held in registers required by law and other lists and registers relating to the functions of the authority.

The services we offer.
Advice and guidance, booklets and leaflets, transactions and media releases. A description of the services offered.

The classes of information will not generally include:

- Information the disclosure of which is prevented by law, or exempt under the Freedom of Information Act, or is otherwise properly considered to be protected from disclosure.
- Information in draft form.

- Information that is no longer readily available as it is contained in files that have been placed in archive storage, or is difficult to access for similar reasons.

The method by which information published under this scheme will be made available

The authority will indicate clearly to the public what information is covered by this scheme and how it can be obtained.

Where it is within the capability of a public authority, information will be provided on a website. Where it is impracticable to make information available on a website or when an individual does not wish to access the information by the website, a public authority will indicate how information can be obtained by other means and provide it by those means.

In exceptional circumstances some information may be available only by viewing in person. Where this manner is specified, contact details will be provided. An appointment to view the information will be arranged within a reasonable timescale.

Information will be provided in the language in which it is held or in such other language that is legally required. Where an authority is legally required to translate any information, it will do so.

Obligations under disability and discrimination legislation and any other legislation to provide information in other forms and formats will be adhered to when providing information in accordance with this scheme.

Charges which may be made for information published under this scheme

The purpose of this scheme is to make the maximum amount of information readily available at minimum inconvenience and cost to the public. Charges made by the authority for routinely published material will 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 information subject to a charging regime specified by Parliament.

Charges may be made for actual disbursements incurred such as:

- photocopying
- postage and packaging
- the costs directly incurred as a result of viewing information

Charges may also be made for information provided under this scheme where they are legally authorised, they are in all the circumstances, including the general principles of the right of access to information held by public authorities, justified and are in accordance with a published schedule or schedules of fees which is readily available to the public.

Charges may also be made for making datasets (or parts of datasets) that are relevant copyright works available for re-use. These charges will be in accordance with the terms of the Re-use of Public Sector Information Regulations 2015, where they apply, or with regulations made under section 11B of the Freedom of Information Act, or with other statutory powers of the public authority.

If a charge is to be made, confirmation of the payment due will be given before the information is provided. Payment may be requested prior to provision of the information.

Written requests

Information held by a public authority that is not published under this scheme can be requested in writing, when its provision will be considered in accordance with the provisions of the Freedom of Information Act.

Horton Parish Council

Data Map – Assertion 10 (Digital and Data Compliance)

This Data Map is prepared to demonstrate Horton Parish Council's compliance with Assertion 10 of the Annual Governance and Accountability Return (AGAR) 2025/26, relating to digital and data governance. It outlines the categories of personal data processed by the Council, their purpose, lawful basis, and the measures in place to protect and manage that data in accordance with the UK GDPR and Data Protection Act 2018.

Category of Data	Purpose of Processing	Lawful Basis (UK GDPR)	Data Subjects	Where Data Is Held / Stored	Access & Sharing	Retention Period	Security Measures
Councillor contact details (names, addresses, emails, declarations)	To enable lawful council business, publish contact details and manage declarations of interest	Public Task / Legal Obligation	Elected and co-opted councillors	Council's secure drive, official council email system, website (public contact details only)	Clerk, councillors, Monitoring Officer (interests)	As long as individual holds office + 1 year	Password-protected storage, .gov.uk email, limited access.
Employee records (contracts, payroll, appraisals, leave)	Employment administration and legal obligations	Contract / Legal Obligation	Clerk, employees	HMRC online account. Parish Council external hard drive/exclusive laptop	Clerk, HMRC	6 years after employment ends	Password protected storage/ external hard drive, secure deletion.

Created: April 2026
Approved: May 2026 by Full Council

Resident correspondence (emails, letters, online forms)	To respond to queries, service requests, or complaints	Public Task / Consent	Residents, service users	Clerk's council email, contact form system	Clerk, relevant Councillor	2 years (or until resolved)	Council domain email only, antivirus, restricted access
Supplier & contractor data (invoices, bank details, contracts)	To manage payments and procurement	Contract / Legal Obligation	Contractors, suppliers	Accounting software, Council's secure drive, official council email system	Clerk, RFO, internal & external auditors	7 years (financial records)	Password protection, restricted drive access
Financial records (budgets, payments, receipts, audits)	Financial management and statutory reporting	Legal Obligation	Clerk, RFO, councillors	Accounting system, council network	Clerk, RFO, auditors, HMRC	7 years	Password protection cloud and external backups, limited access
Website content & accessibility logs	To provide public information and meet accessibility duties	Public Task / Legal Obligation	Members of the public	Council website	Clerk, web administrator	Ongoing	Accessibility compliance checks, secure hosting
Meeting minutes, agendas, recordings	Statutory record of council business	Public Task / Legal Obligation	Councillors, residents, officers	Website (public copies), secure drive	Clerk, councillors, public (published versions)	Permanent	Version control, backups, redaction of personal data

Planning and consultation responses	To respond to statutory consultations	Public Task	Residents, developers, consultees	Clerk's drive, email	Clerk, councillors, planning authority	2 years	Secure network storage
Trust fund / charity data (if sole trustee)	Manage assets and fulfil trustee duties	Legal Obligation	Trustees, beneficiaries	Clerk's records, accounting system	Clerk, trustees, auditors	7 years (financial), permanent (assets)	Secure storage, backups
Data protection requests (SARs, FOIs)	To comply with information rights	Legal Obligation	Residents, data subjects	Council's secure drive, official council email system	Clerk, councillors (if required)	3 years	Secure log, restricted access

Supporting Governance Measures

To fully comply with Assertion 10, Horton Parish Council maintains the following governance measures:

- Data Protection Policy (UK GDPR / DPA 2018)
- Privacy Notice
- Records Retention Policy
- IT & Email Use Policy (requiring council-owned domain e.g. horton-somerset-pc.gov.uk)
- Website Accessibility Statement (WCAG 2.2 AA)
- Data Breach Procedure
- Freedom of Information & Publication Scheme

Horton Parish Council – Accessibility Statement 2026 -myparishcouncil

We are constantly working to make our website as accessible and usable as possible.

AbilityNet provides guidance about how to:

- make your mouse easier to use (opens in new window)
- use your keyboard instead of a mouse (opens in new window)
- talk to your device (opens in new window)
- make your device talk to you (opens in new window)
- make text larger (opens in new window)
- change your colours (opens in new window)
- magnify the screen (opens in new window)

Code

Our website has been developed to best practice coding conventions following World Wide Web Consortium (W3C) Web Accessibility Initiative (WAI) Web Content Accessibility Guidelines 2.2 (WCAG 2.2) and successfully XHTML 1.0 strict valid.

Consistent page headings and titles

A consistent heading structure has been used so that page information is compatible with access technology.

Browsers

The following browsers have been tested for compatibility:

- Internet Explorer (Windows) v7.0 to 9.0
- Google Chrome
- Firefox (Windows and Mac) v2.0 and 12.0
- Safari (Mac) v4.v5
- Opera v9 - 11

Alternative formats

If you would like a publication in an alternative format please contact us through our general enquiries form.

Leave feedback

We are always happy to receive feedback. Please use our online feedback form to let us know about any problems you have had or email our website team.

Horton Parish Council

Accessibility Statement April 2026

The website is operated by the Parish Council and we want as many people as possible to access it. For example, that means that you should be able to:

- Change colours, contrast levels and fonts via the helpful plugins
- Zoom in up to 300% without the text spilling off the screen.
- Navigate most of the website using just a keyboard
- Navigate most of the website using speech recognition software
- Listen to most of the website using a screen reader (including the most recent versions of JAWS, NVDA and Voiceover)

We have also made the website text as simple as possible to understand

AbilityNet has advice on making your device easier to use if you have a disability.

How Accessible this Website is:

The website is partially compliant with Web Content Accessibility Guidelines (WCAG) 2.2 AA Standards due to the non-compliances below

Non-Accessible Content

We know that some parts of this website are not fully accessible. The content listed below is non-accessible for the following reasons:

- you cannot modify the line height or spacing of text
- most older PDF documents are not fully accessible to screen reader software
- live video streams do not have captions
- you cannot skip to the main content when using a screen reader
- there's a limit to how far you can magnify maps

Non Compliance with the accessibility regulations

- Maps display by Google Maps – we don't control how Google Maps displays information, but where possible we provide addresses within the web page's text (via HTML). When Google makes their map output accessible, we will update our technology accordingly.
- Pictures of event or information posters, when provided by a third party – where possible we provide the information from the picture, within the web page's text (via HTML). We will encourage all providers of these pictures to provide accessible alternatives in future.
- Some images on the council news update page do not have a text alternative, so people using a screen reader cannot access the information. This fails WCAG 2.2 success criterion 1.1.1 (non-text content). We are addressing any missing ALT tags. When we publish new content we'll make sure our use of images meets accessibility standards.
- Some PDFs published since September 2018 are not in an accessible format, so people using a screen reader cannot access the information. When we publish new content we'll make sure our use of PDFs meets accessibility standards.
-

Disproportionate Burden

Navigation and accessing information

It's not always possible to change the device orientation from horizontal to vertical without making it more difficult to view the content.

It's not possible for users to change text size without some of the content overlapping.

Interactive Maps

Maps displayed by Google Maps – as above

Content that's not within the scope of the accessibility regulations

- Some documents are created by third parties or using third party software. Where this is the case we will endeavour to convey the information contained in the document in an accessible way.
- Live video streams do not have captions. This fails WCAG 2.2 success criterion 1.2.4 (captions – live). We do not plan to add captions to the live video streams because live video is exempt from meeting the accessibility regulations.

What to do if you Cannot Access Parts of this Website

If you need information on this website in a different format like accessible PDF, large print or easy read please contact:

Email: clerk@horton-somerset-pc.gov.uk

Call: 07471341433

We'll consider your request and respond as soon as possible.

Reporting Accessibility Problems with this Website

We're always looking to improve the accessibility of this website. If you find any problems not listed on this or think we're not meeting accessibility requirements, contact the Clerk giving the page title and the nature of the problem.

9 Redgate Park
Crewkerne
TA187NL

Email: clerk@horton-somerset-pc.gov.uk
Tel: 07471341433

Enforcement Procedure:

The Equality and Human Rights Commission (EHRC) is responsible for enforcing the Public Sector Bodies (Websites and Mobile Applications) (No.2) Accessibility Regulations 2018 (the 'accessibility regulations'). If you're not happy with how we respond to your complaint, contact the Equality Advisory and Support Service (EASS).

Technical Information about this Website's Accessibility:

Horton Parish Council is committed to making its website accessible, in accordance with the Public Sector Bodies (Website and Mobile Applications) (No.2) Accessibility Regulations 2018.

How we tested the site
Self-evaluation in April 2026

What are we doing to improve accessibility
To improve and maintain accessibility we will re-test the site on an annual basis and provide staff training to help ensure that all new content added meets accessibility criteria