

Information Technology Policy

1. Introduction

- 1.1 This policy sets out how Lyme Regis Town Council manages and protects its information technology (IT) systems, electronic communications, and digital information. It should be read in conjunction with the Council's Information Policy and Social Media Policy. Together, these policies establish the framework for the secure, lawful, and appropriate use of council information, technology, and communications.
- 1.2 This policy applies to:
 - 1.2.1 All individuals who use Lyme Regis Town Council's IT resources, including councillors, employees, contractors, and volunteers who use IT systems or devices for council business.
 - 1.2.2 All council-owned devices, systems, software, and online services.
 - 1.2.3 Any personal devices used to access or process council information.
- 1.3 The aim of this policy is to ensure the Council's digital activities are secure, lawful, and transparent, in accordance with the Practitioners' Guide 2025 and Assertion 10: Digital and Data Compliance within the Annual Governance Statement.

2. Hardware

- 2.1 Council computer equipment is provided for council purposes; however, limited personal use is permitted. 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.
- 2.2 All staff, councillors, and other authorised users must lock their computers when leaving their desks to prevent unauthorised access. This applies to all council and personal devices used for work. Failure to comply may lead to disciplinary action against staff.
- 2.3 All computer and other electronic equipment supplied should be always treated with great care. Any loss, theft or damage should be reported immediately. If the loss or damage is due to an act of negligence, the individual responsible may be liable to meet the first 50% of the loss/damage.
- 2.4 Council-owned equipment, including laptops, tablets, printers, mobile phones etc., remains the property of the council. Users must not install software or apps without prior authorisation.
- 2.5 All council-owned devices must be configured to receive automatic security updates where possible. Users must not disable update mechanisms or delay critical security updates without authorisation.

- 2.6 Personal disks, USB stick, CDs, DVDs, data storage devices, etc cannot be used on council computers without the prior approval of the clerk.
- 2.7 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 always kept with or near the user; should not be left unattended when away from council premises and should never be left in parked vehicles.

3. Equipment – Use of own devices

- 3.1 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.
- 3.2 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. The following data must never be accessed or processed on a personal device: personal data relating to councillors, staff, and other authorised users, associates, residents, external stakeholders.
- 3.3 Any council information accessed on personal devices must be protected by appropriate security measures, including device passwords, encryption where available, and up-to-date security software.
- 3.4 If personal removable media is 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.

4. Health and safety

- 4.1 Users of display screen equipment must comply with the Council's Health and Safety Policy.
- 4.2 The council will provide workstation assessments, eye tests, and other support as required by applicable health and safety legislation.

5. Password and Authentication Policy

- 5.1 Initial user account passwords will be generated by the IT provider. Default passwords provided by vendors or the IT provider must be changed immediately upon installation or setup.
- 5.2 Access to Passwords
 - 5.2.1 Passwords are personal and must not be shared under any circumstances.
 - 5.2.2 Only the assigned user of an account may access or use the associated password.

5.2.3 In exceptional cases, e.g., incident response or employee leaving, access to system credentials may be granted to authorised personnel from the IT provider with appropriate approvals and logging.

5.3 Password Storage and Management

5.3.1 Passwords must not be stored in plain text or written down in insecure locations.

5.3.2 Passwords must be stored using a council-approved, encrypted password manager, e.g., Keeper, LastPass, or Edge password manager.

5.4 Password Change Requirements

5.4.1 Immediately change password if compromise is suspected.

5.5 Multi-Factor Authentication

5.5.1 Multi-factor authentication (MFA) must be enabled on all council systems where this functionality is available, particularly for email accounts, cloud-based services, administrator accounts, and remote access systems.

5.6 Password Access Control and Logging

5.6.1 All access to administrative or shared credentials must be logged and auditable.

5.6.2 Attempts to access unauthorised passwords will be treated as a security incident.

5.7 Responsibility

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

5.7.2 The IT security provider is responsible for:

5.7.2.1 Managing system/service credentials.

5.7.2.2 Enforcing password policies. Auditing and monitoring password-related security practices.

6. Monitoring

6.1 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. Monitoring will be conducted in accordance with the Data Protection Act and General data protection regulations (GDPR).

6.2 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.

- 6.3 The information gathered through monitoring will be retained only long enough for any breach of this policy to become known and for any investigation to be conducted.
- 6.4 Further information regarding data protection rights is available in the council's Information Policy.
- 6.5 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.
- 6.6 Cyber Security Incidents
 - 6.6.1 Any suspected cyber security incident must be reported immediately to the town clerk and, where appropriate, the council's IT provider.
 - 6.6.2 Cyber security incidents include phishing emails, malware infections, unauthorised access attempts, lost or stolen devices, accidental disclosure of information, and suspicious system activity.
 - 6.6.3 Users must not attempt unauthorised investigation or remediation of security incidents.

7. Remote Working

- 7.1 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.
- 7.2 Council information and equipment must be protected from unauthorised access when working away from council premises. Printed documents, electronic files and devices must be securely stored and must not be left unattended.
- 7.3 Where possible, the ability to remotely wipe any mobile devices that process sensitive information should be retained in the case of loss or theft.
- 7.4 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 always use this when accessing such data away from the office.

8. Email

- 8.1 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.

- 8.2 Limited personal use is permitted, provided it does not interfere with work responsibilities or violate any part of this policy. All users must adhere to ethical standards, respect copyright, and intellectual property rights, and avoid accessing inappropriate or offensive content.
- 8.3 Be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links.
- 8.4 All council business must be conducted using council-approved email accounts. Personal email accounts must not be used for council business.
- 8.5 Access to council email accounts will be withdrawn when a councillor or employee leaves their role, and records may be retained by the council.

9. Use of the Internet

- 9.1 Users must comply with the Copyright, Designs and Patents Act 1988 and must not download, copy or share copyrighted material without appropriate authorisation. Councillors, staff, and other authorised users are required to refer to the Copyright, Designs and Patents Act 1988 in cases of uncertainty.
- 9.2 Downloading and sharing copyrighted material without proper authorisation is prohibited.
- 9.3 The council does not permit the registration of any new domain names or trademarks relating to the council's names or products, unless authorised to do so. Nor should users add links from any of the council's web pages to any other external sites without authorisation.
- 9.4 Special rules apply to the processing of personal and sensitive personal data. For further guidance on this, see the council's Information Policy.

10. Use of social media

- 10.1 Social media includes blogs, collaborative sites, e.g. Wikipedia, multimedia platforms, e.g. YouTube, social networking sites, e.g. Facebook, LinkedIn, X, Instagram, TikTok, virtual environments, mobile communications, and traditional media such as television and newspapers. Care must be taken when using social media at any time, whether on council systems or personal devices.
- 10.2 The council's official social media accounts are managed by the assistant town clerk as authorised by the council.
- 10.3 Staff and councillors must not represent personal views as those of the council.
- 10.4 Posts and comments must be factual, respectful, and non-political.
- 10.5 Inappropriate or offensive content must be reported to the town clerk for moderation or removal.

- 10.6 Use of messaging platforms, e.g. WhatsApp, Facebook Messenger, for council business must be limited to administrative coordination and not decision-making.
- 10.7 Councillors, staff and authorised users must not misrepresent their role within the council, disclose confidential information, or publish content that could bring the council into disrepute. These requirements continue after an individual leaves office or employment.
- 10.8 It is important to note that external stakeholders contact details and information remain the property of the council.

11. Misuse

- 11.1 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.

12. AI (Artificial Intelligence)

12.1 Scope

- 12.1.1 Artificial Intelligence (AI) refers to the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings.
- 12.1.2 Lyme Regis Town Council recognises the benefits and risks associated with AI and is committed to a risk-based approach to its implementation and use, including:
- 12.1.3 Assessing and mitigating risks associated with the use of AI.
- 12.1.4 This policy ensures any use of AI supports the council's commitment to transparency, accountability, and service to the public.
- 12.1.5 This framework applies to all council employees, councillors, contractors, consultants or third parties providing AI-driven services on behalf of the council, and AI systems used for communication, document generation, data analysis, or public engagement.

12.2 Guiding principles

12.2.1 The use of AI within the council must be:

- 12.1.1.1 Transparent – AI assisted content or communications must be clearly labelled or explained if relevant to public-facing work.
- 12.1.1.2 Ethical and inclusive – AI must not be used in ways that discriminates, misleads, or reinforces bias. The council will seek fair and inclusive outcomes in its use of technology.
- 12.1.2.3 Human-centred – AI will assist, not replace, human judgement. Council officers remain responsible for reviewing and approving AI-generated outputs.

- 12.1.2.4 Compliant with Data Protection Law – all AI use must comply with the UK GDPR, Data Protection Act 2018, and Freedom of Information Act. No personal data should be entered into publicly available AI platforms without appropriate safeguards.
- 12.1.2.5 AI-generated content must be reviewed by a suitably authorised officer or councillor for accuracy, completeness, and appropriateness before use or publication.

12.3 Permitted use

12.3.1 Lyme Regis Town Council may use AI for:

- 12.3.1.1 drafting reports, minutes, and publicity materials (with human review)
- 12.3.1.2 analysing trends in local feedback or surveys
- 12.3.1.3 supporting accessibility, e.g. speech-to-text tools, translation
- 12.3.1.4 improving efficiency of internal processes.

12.4 Prohibited use

12.4.1 AI must not be used for:

- 12.4.1.1 making decisions that have legal or significant effects on individuals
- 12.4.1.2 any form of surveillance or facial recognition
- 12.4.1.3 generating or spreading misinformation
- 12.1.1.4 entering sensitive or confidential data into unsecured or public AI platforms
- 12.1.1.5 AI must not be used as the sole basis for decisions affecting individuals, council services, or statutory functions.

12.5 Oversight and training

- 12.5.1 The town clerk will oversee AI-related use and compliance.
- 12.5.2 Council staff and councillors will receive guidance/training as needed.
- 12.5.3 Any significant implementation of AI technology must be approved by the council in consultation with the council's IT provider.

12.6 Public transparency

- 12.6.1 The council will maintain openness about its use of AI and respond to public queries accordingly.
- 12.6.2 AI-generated content that is published or shared with the public will be noted or acknowledged as appropriate.

13. Monitoring and Review

- 13.1 This policy will be reviewed annually or in response to changes in regulation or technology. Breaches of this policy may lead to restrictions on AI use or disciplinary action, where applicable.

14. Leaving Office or Employment

- 14.1 Upon leaving office or employment, individuals must:
 - 14.1.1 return all council-owned equipment.
 - 14.1.2 surrender council access credentials where required.
 - 14.1.3 remove council data from personal devices and accounts.
 - 14.1.4 cease using council systems and services.
 - 14.1.5 confirm deletion of council information held outside approved council system
 - 14.1.6 comply with continuing confidentiality obligations.

15. Contacts

- 15.1 For IT related enquiries or assistance, staff and councillors can contact Dorset Council ICT desk on 01305 224062.
- 15.2 For suspected security breaches, staff and councillors can contact the town clerk on 01297 445175.

16. Privacy

- 16.1 Lyme Regis Town Council is committed to protecting personal information and ensuring all processing of personal data complies with the UK GDPR, the Data Protection Act 2018, and any other applicable legislation.
- 16.2 Councillors, staff, contractors, and authorised users must:
 - 16.2.1 only access personal data where necessary for their role.
 - 16.2.2 ensure personal information is accurate, secure, and kept confidential.
 - 16.2.3 report any actual or suspected data breach immediately to the town clerk.
 - 16.2.4 only use council-approved systems and services for storing or processing council information.
 - 16.2.5 comply with the council's Information Policy, Privacy Notices, and Information Policy.
- 16.3 Personal data must not be disclosed to unauthorised persons or used for purposes unrelated to council business.

17. Audio Recordings

- 17.1 Audio recordings made for council purposes, including the recording of council meetings, training sessions, interviews, or dictated notes, must be managed in accordance with the council's Information Policy and Retention Schedule.
- 17.2 Audio recordings must only be made where there is a legitimate council purpose.
- 17.3 Individuals should be informed where meetings or events are being recorded.

- 17.4 Recordings must be stored securely and only accessed by authorised persons.
- 17.5 Recordings must not be shared externally without appropriate authority.
- 17.6 Where recordings are used to assist in producing minutes or transcripts, the recording should be deleted in accordance with the council's retention requirements once it is no longer required.
- 17.7 Any AI-generated transcript must be reviewed for accuracy before being relied upon for council business.

18. CCTV

- 18.1 Where the council operates or manages CCTV systems, these systems must be used for lawful purposes, including public safety, crime prevention, the protection of council assets, and the investigation of incidents.
- 18.2 CCTV footage must be stored securely and access restricted to authorised individuals.
- 18.3 CCTV recordings will be retained only for as long as necessary and in accordance with the council's retention requirements.
- 18.4 Requests for CCTV footage must be managed in accordance with data protection legislation and the council's relevant policies.
- 18.5 CCTV systems must not be used to monitor individuals unreasonably or in a manner inconsistent with their intended purpose.
- 18.6 Appropriate signage must be displayed wherever CCTV is in operation.

19. Microsoft Teams

- 19.1 Microsoft Teams is an approved communication and collaboration platform for council business.
- 19.2 Users must:
 - 19.2.1 use Teams professionally and in accordance with this policy.
 - 19.2.2 communicate respectfully and appropriately at all times.
 - 19.2.3 ensure confidential or personal information is shared only with authorised recipients.
 - 19.2.4 use council-issued accounts when participating in council business
 - 19.2.5 comply with records management and retention requirements.
- 19.3 Meeting organisers are responsible for:
 - 19.3.1 ensuring meeting invitations are issued appropriately.
 - 19.3.2 controlling access to meetings where confidential information may be discussed.

19.3.3 notifying participants when meetings are being recorded

19.3.4 ensuring recordings and transcripts are managed in accordance with council policies.

19.4 Teams messaging, files, recordings, and transcripts may constitute council records and may be subject to retention requirements, Freedom of Information requests, legal disclosure obligations, and monitoring by the council where permitted by law.

19.5 Where Microsoft Teams recordings are transcribed using AI-powered tools, users must ensure confidential or personal information is not inappropriately disclosed and that any transcript is checked for accuracy before use.

Implementation date: 9 September 2026

Review Date: September 2029

John Wright
Town clerk
September 2026