Data Security and Bring Your Own Device Policy

Date **please insert date of adoption** (which must match the resolution number)

Edition No and Date 1 / XX.XX.2024

Replaces Data Protection Policy 30.03.2017 *to be discarded*

Policy Maker Jon Short, Deputy Town Clerk

Responsibility Policy and Finance

Resolution Number **please insert resolution number from minutes (DD.MM.YY. / Min.Min.Min.)**

Review Cycle Every 3 years or earlier in the event of legislative change

This information pack contains:

Data Security and Bring Your Own Device Policy
Policy 1: Data Security and Bring Your Own Device Policy
Appendix 1: Social media, instant messaging and collaboration services that are authorised for use in the organisation

For reviews with no changes or minor changes only – agreed by Town Clerk and Deputy Town Clerk.
N/A

Littlehampton Town Council

Data Security and Bring Your Own Device Policy

This data security and bring your own device policy sets out the procedures we have put in place to maintain the security of personal data and other data within our organisation.

We are Littlehampton Town Council a council in England. Our contact details are The Manor House, Church Street, Littlehampton, West Sussex, BN17 5EW, 01903 732063, ltc@littlehampton-tc.gov.uk

We are a data controller for personal data as defined by all applicable data protection and privacy laws including, but not limited to, the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (the "UK GDPR"), as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 as amended, and any successor legislation (the "Data Protection Legislation").

This policy is binding on all employees, councillors and volunteers ("User" or "Users") of Littlehampton Town Council ("The Organisation") in order to protect Personal or other Data ("Personal Data" or "Data") processed by the organisation.

It applies to all organised filing systems be they computer based, paper based or any other such method of organising information which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis ("Filing Systems").

1. **Person Responsible**

1.1. The Town Clerk is responsible for the ongoing compliance monitoring of this and other policies that are designed to achieve compliance with the Data Protection Legislation. ("the person responsible for data protection").

1.2. No user within the organisation shall deviate from this policy without written authorisation from the person responsible for data protection.

2. **Acceptable Use**

2.1. Data shall only be used within the organisation for the purposes of the organisation.

2.2. Data shall not be shared with third parties or other data controllers without a data sharing agreement having been finalised and signed by the person responsible for data protection.

2.3. Only data processors that have contracts with the organisation that have been authorised by the person responsible for data protection shall be used.

2.4. Users processing data on behalf of the organisation are reminded of the need to keep proper records in accordance with this and other policies designed to maintain compliance with the data protection legislation and the freedom of information act.

3. Passwords

3.1. Users processing data on behalf of the organisation on systems that require passwords shall use a password that conforms to the following:

3.1.1. Is sufficiently complex and is made up of at least three random unconnected words.

3.1.2. Is not used for other logins be they personal or professional.

3.1.3. Is not disclosed to anyone or written down.

3.2. Passwords must not be shared amongst the organisation's users. If a user has a legitimate need for data that they cannot access with their own password then the person responsible for data protection should be advised so that access levels may be changed if appropriate.

3.3. Users should be aware that no one will ever ask a user for their password. Any request for a password to be disclosed should be reported to the person responsible for data protection immediately.

3.4. Where multi factor authentication is available it shall be used.

3.5. Multi factor authentication codes must not be disclosed to others or shared amongst the organisation's users.

3.6. Users should be aware that no one will ever ask a user for a multifactor authentication code. Any request for a multifactor authentication code to be disclosed should be reported to the person responsible for data protection immediately.

4. Email and cloud storage

4.1. The organisation does not allow users to process the organisation's data using their own personal email accounts.

4.2. The organisation does ~~not~~ allow users to access email or cloud storage accounts provided by the organisation using their own personally owned computers, laptops, or other mobile devices, however the data must remain in the cloud and not be downloaded in permanent form to the users device.

5. Social Media and Instant Messaging

5.1. The organisation's data shall not be uploaded, posted or otherwise transferred to social media (including but not limited to Facebook, Twitter, Instagram, TikTok, YouTube) without the authorisation of the person responsible for data protection.

5.2. The organisation's data shall not be uploaded, posted or otherwise transferred to instant messaging or collaboration services (including but not limited to Whatsapp, Teams, Skype, Facebook Messenger, Slack, Google Workspace) without the authorisation of the person responsible for data protection.

5.3. Social media, instant messaging and collaboration services that are authorised for use in the organisation are listed in appendix A.

6. Physical Security

6.1. Servers shall be located in locked rooms.

6.2. Computers shall not be left unattended without the screen being locked or the user logged out.

6.3. Paper files shall be kept in locked filing cabinets or locked filing rooms.

6.4. Documents no longer required shall be disposed of via secure means such as cross cut shredding or commercial document destruction.

6.5. Where documents are disposed of by commercial document destruction they shall be disposed of securely and a certificate of destruction obtained.

7. System Security

7.1. Users of the organisation's data shall be granted the appropriate level of access to cloud or computer systems to allow them to undertake their duties.

7.2. Routine working with administrator rights is not allowed.

7.3. Computer files and records shall be kept within the organisation's cloud storage system.

7.4. USB sticks and other removable media shall not be used on the organisation's computer system.

7.5. Storage media on servers shall be encrypted.

7.6. Servers shall be backed up using a minimum 3-2-1 strategy:

7.6.1. 3 copies of the data.

7.6.2. On 2 different media types.

7.6.3. With 1 backup off site.

7.7. Cloud servers shall be backed up by the cloud service provider in a way that is not less robust than a 3-2-1 strategy.

7.8. Backups shall be subject to twice yearly recovery testing to ensure that they are fit for purpose from April 2025. ~~.~~

7.9. Software including operating systems shall be regularly kept up to date and patched with the latest security updates from its developers.

7.10. WiFi networks shall have a minimum WPA2 encryption standard if they are used to transmit data.

7.11. Public WiFi provided by the organisation shall be firewalled in such a way that the organisation's data is segregated from it.

7.12. Regular ~~penetration testing~~ open port testing at least 2 times a year shall be undertaken on all firewalls ~~and computer network security systems~~ from April 2025. ~~.~~

7.13. Suitable anti virus software and anti malware software shall be used on all of the organisations computers, laptops or other mobile devices.

7.14. The organisation does not allow users to join their own personally owned computers, laptops, or other mobile devices to the organisation's computer network used for processing data.

7.15. When electronic documents, files or records are no longer required they shall be deleted in such a way as to put the data beyond use. Data will be deemed to be put beyond use if:

7.15.1. The data is not able to be used to inform any decision in respect of any individual or in a manner that affects the individual in any way, and

7.15.2. The organisation does not give any other organisation access to the data, and

7.15.3. The organisation surrounds the personal data with appropriate technical and organisational security, and

7.15.4. The organisation commits to permanent deletion of the information if, or when, this becomes possible.

8. Breaches

8.1. Any suspected breach of the confidentiality integrity or availability of personal data within our organisation shall be immediately and within 1 hour notified in writing to the person responsible for data protection.

8.2. Breaches of the confidentiality integrity or availability of personal data within our organisation shall be investigated immediately by the person responsible for data protection and a determination made as to the level of risk of data being breached, the number of individuals involved, the severity of any breach and if the Information Commissioner's Office should be notified. This investigation must take a maximum of 72 hours from the first discovery of the breach.

8.3. No user should try to rectify a breach without first informing and getting authorisation from the person responsible for data protection.

9. Updates to this policy

9.1. This policy shall be reviewed ~~annually~~ every three years by the person responsible for data protection.

9.2. This policy shall be reviewed if Littlehampton Town Council makes changes to the organisations Privacy Notice or if there are changes to how the organisation processes data or the data protection legislation changes.

9.3. This policy was last updated on [date].

10. Implementation

10.1. This policy takes effect from [date] and is not retroactive.

Appendix 1
Social media, instant messaging and collaboration services that are authorised for use in the organisation

Company	Product	Processor or controller	Reason
Meta	Facebook	Controller	Marketing
X Corp.	X (Twitter)	Controller	Marketing
Meta	Instagram	Controller	Marketing
Microsoft	Teams	Controller	Virtual meetings