Bexhill-on-Sea Town Council Dropbox Usage Policy

1. Purpose
This policy governs the use of the Dropbox online server by Bexhill-on-Sea Town Council to ensure secure, efficient, and compliant handling of documents and data.

2. Scope
This policy applies to all employees, elected members, contractors, and any other authorized individuals using the Council's Dropbox account for the storage and sharing of Council-related files.

3. Objectives
The purpose of using Dropbox is to:

- Facilitate secure storage and sharing of Council documents.
- Enhance collaborative work between council staff.
- Ensure access to critical files while working remotely.

4. Responsibilities

- **Council Staff:** Must adhere to this policy, safeguarding login credentials and ensuring that data stored or shared is appropriate and within the scope of Council business.
- **IT Administrator:** Responsible for managing user access, maintaining security settings, and monitoring usage.
- **All Users:** Must ensure that any files uploaded or shared comply with Council policies, including Data Protection regulations.

5. Access and Permissions

- Access to Dropbox accounts will be granted by the Town Clerk or authorised administrators.
- Users will be assigned appropriate permissions based on their roles (e.g., view-only, editor, admin).
- Sharing files with external parties should be restricted and must be approved by a senior council member or administrator.

6. Acceptable Use

- Dropbox must only be used for official Council business.
- Personal files or data unrelated to Council activities must not be uploaded to the Dropbox account.
- Users must ensure that all documents are clearly labelled and organized in the correct folders.

7. Data Security

- Sensitive or confidential data should only be stored in designated secure folders.
- Users must not share Dropbox links or credentials outside of authorised personnel without prior approval.

- Regular backup checks should be conducted to ensure no data loss in case of server issues or accidental deletions.

8. Data Protection & Privacy

- The Town Council must comply with the Data Protection Act 2018 (UK GDPR). Personal and sensitive information must be handled in accordance with data protection principles.
- Files containing personal data should be encrypted or stored in secure, restricted-access folders.
- User access logs will be maintained for auditing purposes.

9. File Retention & Deletion

- Files must be regularly reviewed, and obsolete or irrelevant files should be deleted or archived following the Council's data retention policy.
- Deletion of sensitive files should be irreversible (using Dropbox's permanent delete function) to prevent unauthorized recovery.

10. Incident Reporting

- Any data breaches, unauthorised access, or loss of files must be reported immediately to the Council's IT team and Data Protection Officer (DPO).
- In the case of a data breach involving personal information, the DPO must follow the appropriate reporting procedures to the Information Commissioner's Office (ICO).

11. Training

- All users must undergo mandatory training on how to use Dropbox securely and in compliance with Council policies.
- Refresher training will be offered annually or as needed.

12. Monitoring & Compliance

- The Town Council reserves the right to monitor Dropbox usage to ensure compliance with this policy.
- Misuse of Dropbox, including unauthorised sharing of files, can result in disciplinary action.

13. Policy Review

- This policy will be reviewed annually or whenever significant changes are made to Dropbox's functionality, UK data protection laws, or the Town Council's working practices.

14. Approval This policy was approved on XXXXX