BEXHILL-ON-SEA TOWN COUNCIL
IT AND CYBERSECURITY POLICY
FOR APPROVAL

1. Introduction

1.1. Bexhill-on-Sea Town Council has a duty to ensure the proper security and privacy of its computer systems and data. All users have some responsibility for protecting these assets.
1.2. The Town Clerk is responsible for the implementation and monitoring of this policy but may delegate that responsibility to another officer.
1.3. Line managers have a responsibility to ensure that staff they supervise comply with this policy.

General Principles

1.4 All employees, members and other users should be aware of the increasingly sophisticated scams and risks posed to cybersecurity and when in any doubt should seek guidance from the Town Clerk. As a general rule, users will never be asked to share passwords by email and users should be aware of odd language used in emails which may indicate a fraudulent email.

1.5 All employees, members and other users of council IT equipment must be familiar with and abide by the regulations set out in the council's 'Data Protection and Document retention policy.

1.6 All council devices will have up-to-date antivirus software installed and this must not be switched off for any reason without the authorisation of the Town Clerk.

1.7 All users are reminded that deliberate unauthorised use, alteration, or interference with computer systems, software or data is a breach of this policy and in some circumstance may be a criminal offence under the Computer Misuse Act 1990.

1.8 All software installed on council devices must be fully licensed and no software should be installed without authorisation from the Town Clerk.

Training

1.9 Employees and volunteers will be provided with regular cybersecurity training as is appropriate for their role and level of systems access.

1.10 Members will be provided with a brief overview of cybersecurity measures as part of induction and may be provided with more in-depth training as required.

2. GENERAL IT POLICY

Employees/Volunteers

2.1 All employees will be assigned a council email address, as appropriate. Volunteers may also be assigned a council e-mail address where necessary.

2.2 Personal use of Council IT equipment is permitted but should be kept to a minimum during working hours. Reasonable use of the internet during working hours is permitted.

2.3 The Council reserves the right to monitor all activity on company devices. This includes monitoring of email activity and internet usage for the purposes of ensuring compliance with our policies and procedures and of ensuring compliance with the relevant regulatory requirements. Information acquired through such monitoring may be used as evidence in disciplinary proceedings. Monitoring usage will mean processing personal data.

Members

2.4 All members will be provided with a council email address and must use this for all council business.

2.5 Members are reminded that any email sent or received in their capacity as Town Councillor is Council data and any emails may have to be disclosed following requests under the Data Protection Act or Freedom of Information Act. This includes emails on Personal Accounts when acting as a Councillor.

2.6 A copy of all email received on the councillor email accounts is kept on the server in line with the council's Data Protection and Retention Policy.

2.7 Members using social media in their capacity as councillors must make it clear they are speaking in a personal capacity and not representing the view of the council.

2.8 Members should ensure they are adhering to the Council's code of conduct when using social media.

2.9 Members must ensure that any personal devices used to access council systems (including email, websites and data) are password protected, and access is restricted solely to the member.

2.10 In the period between the notice of an election and the election itself (purdah), the Town Council is subject to rules which impact on how it can communicate with the public. Prior to local elections, media releases will not contain a quote from any Member. In these circumstances, where a quote is required, the relevant Officer may be quoted. Once a general election is declared a comparable embargo applies.

2.11 During an election period, Town Council media releases should not deal with controversial issues or report views, proposals or recommendations in a way that identifies them with individual members or groups of members. This ensures that no individual Member gains an unfair advantage by appearing in official publicity.

Website and Social Media

3.1 Officers shall ensure that any websites operated by the council are regularly reviewed to ensure content is accurate and up to date. Website shall also be monitored for unauthorised access or abuse.

3.2 Council social media accounts will be operated by officers. The Town Mayor's official social media accounts may also be operated by the Civic Administrator/Communications Officer.

3.3 All council social media messages must be non-political, uncontroversial and used to promote/highlight the Town.

3.4 Approval must be obtained from the Town Clerk prior to creation of any council websites or social media accounts.

3.5 No information should be published on social media that is not already known to be in the public domain, i.e. available to view on the Town Council's website, contained in public minutes of meetings, stated in Town Council publicised policies and procedures, publicly available on third party websites or hard copy published material or approved by the Town Clerk or Deputy Town Clerk. Members should not reveal any confidential or potentially sensitive information about the Town Council that Members may have accessed in their capacity as a councillor.

3.6 Information that is published on social media should be factual and fair and not bring the council into disrepute.

3.7 Do not publish anything on social media that would be regarded in the workplace as unacceptable.

3.8 Officers using Town Council social media accounts should bear in mind that they will be seen as ambassadors for the Town Council and should always act in a responsible and socially aware manner.

3.9 Generally, comments posted by members on BoSTC social media are individually expressed. It is understood unless stated otherwise that members are commenting individually and not as a Councillor.

3.10 In all cases, at such times where members contribute to discussion on social media posts issued by the Town Council, or where Members use their personal social media accounts in their official capacity as a councillor, Members should always be mindful of the principles applicable to holding public office – integrity, objectivity, accountability, professionalism, honesty and openness.

3.11 Be vigilant and look out for defamatory, discriminatory, abusive or obscene posts or comments from others on the Town Council's social media platforms and report them immediately to the Town Clerk, Deputy Town Clerk or Communications Officer.

3.12 Be aware that, because of Members's public profile as a Town Council member, Members could be regarded as acting in an official capacity when they post any content on Town Council social media platforms or personal social media accounts. Therefore, Members should ensure that any comments posted on behalf of the Town Council are appropriate and information in such comments or posts is correct.

3.13 Be careful if making points which could be deemed 'political' on Town Council social media platforms or personal social media accounts, and avoid being specific or personal about individuals, including other Town Council members.

3.14 Members should not post offensive comments about the Town Council or its Members and Officers, in addition to colleagues, representatives of partner agencies or members of the public. They should not include contact details or photographs of service users or Town Council officers without written consent.

3.15 Members/Officer should not upload, publish or forward links on the Town Council's social media platforms to any abusive, obscene, discriminatory, derogatory or defamatory content. Any Council Member or Officer who feel that they have been intimidated, bullied or harassed, or are

offended by material posted or uploaded should inform the Town Clerk or Deputy Town Clerk immediately.

3.16 Members/Officers should not escalate heated discussions and should, alternatively, attempt to be conciliatory, respectful and state facts to calm the situation and correct any misrepresentations.

3.17 Members/Officers should not discuss topics that may be inflammatory, e.g. politics and religion. Town Council members should be mindful that, although it is acceptable to make political points or canvass votes via Town Council Members' personal social media accounts, this will not be permissible if commenting on behalf of the Town Council.

Password Protection

4.1 All council computers and systems must be password protected to prevent unauthorised access.

4.2 Where possible, two-factors authentication should be utilised.

4.3 Users should ensure that unattended devices are password protected.

4.4 Passwords must conform to the following criteria.

A Minimum eight characters
B Comprise at least one upper case letter, one lowercase letter, one number and one special character.

4.5 Where possible, generic user accounts should be avoided.

4.6 Where users have unique access permissions and/or accounts for systems, these must not be shared with other users.

4.7 Different passwords should be used for different devices and accounts.

4.8 Passwords should be routinely changed.

4.9 Passwords should not be written down or left in unsecure locations.

Portable Devices

5.1 All portable devices (including tablets and mobile phones) must be protected to prevent unauthorised access. This can be by use of passwords, passcodes or other biometric measures as applicable.

5.2 Passcodes must be appropriate for the device and the level of risk that unauthorised access poses to the organisation; where devices can access council data or other systems, passcodes must be unique and not easily accessible.

5.3 Particular care must be taken when using removeable media to transmit data as such media are easily lost or intercepted. Any sensitive information (including personal data, confidential documents or data which could impact on the rights or reputation of any person or organisation including the council) placed on removeable media must be suitably password protected or encrypted.

Incident Reporting

6.1 All members, employees or volunteers must report any incidents which could pose a risk to the council's systems or data security to the Town Clerk without delay. This includes but not limited to:

A – Lost devices
B – Potential risk arising from phishing emails/websites
C – Passwords having been shared
D – Unauthorised access to systems

Misuse of IT

7.1 IT Systems will be monitored for misuse and all misuse is prohibited.

7.2 Misuse includes, but is not limited to:

A. Creation or transmission of any offensive, obscene or indecent images, data or other material or any data capable of being resolved into obscene or indecent images or material.
B. Creation of material which is designed or likely to cause annoyance, inconvenience, or needless anxiety.
C. Creation or transmission of defamatory material
D. Transmission of material which in anyway infringes the copyright of another person
E. Transmission of unsolicited commercial advertising material to networks belonging to other organisations
F. Deliberate actions or activities with any of the following characteristics.
    i. Wasting staff effort or networked resources
    ii. Corrupting or destroying another user's data
    iii. Violating the privacy of other users
    iv. Disrupting the work of other users
G. Other misuse of networked resources by the deliberate introduction of viruses/malware
H. Playing games during work hours
I. Altering the set up or operating perimeters of any computer equipment without authority.

7.3 Unauthorised access, use, destruction, modification and/or distribution of council information, systems or data is prohibited.