Knutsford Town Council

IT Policy

QUALITY
TOWN
COUNCIL

CONTENTS

INTRODUCTION

1.1 The 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 CLAUSES

2.1 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 & Retention Policy'.
2.2 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.
2.3 All council devices should be password protected to prevent unauthorised access.
2.4 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 circumstances may be a criminal offence under the Computer Misuse Act 1990.
2.5 All users should ensure that portable equipment is properly locked away when not in use.
2.6 All software installed on council devices must be fully licensed

EMPLOYEES

3.1 The Town Clerk will assign employees a Council e-mail address as appropriate
3.2 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.
3.3 Software should not be installed without the authorisation of the Town Clerk

MEMBERS

4.1 All members will be provided with a Council e-mail address and should use this for all council business.

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

4.3 A copy of all e-mail received on the Councillor e-mail accounts is kept on the server

4.4 A copy of all e-mail sent from Councillor e-mail accounts on the webmail is kept on the server; it is recommended that members not using webmail to access e-mail should set up a rule to ensure a copy of e-mail is kept on the server.

4.5 Members may borrow a laptop from the Council for Council business

a. The maximum period for the loan is three months
b. The maximum loan period may be extended at the discretion of the Mayor and Town Clerk in exceptional circumstance
c. There is a limit of one machine per household

4.6 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.

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

SOCIAL MEDIA

5.1 Social Media (such as Facebook and Twitter) may be used by the Town Council as part of its means of communication with the community

5.2 All general social media will be operated by council officers

5.3 The Mayor's official social media accounts will be operated by the Mayor and officers

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

COUNCIL WEBSITE(S)

6.1 Council officers should ensure any websites operated by the council are kept up-to-date

6.2 Officers must ensure that the most up-to-date version of the Members' Register of Interests is uploaded to the website

6.3 The website will be monitored for unauthorised access and abuse

MISUSE

All misuse is prohibited including specifically, but not exclusively the following:

7.1 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

7.2 Creation of material which is designed or likely to cause annoyance, inconvenience or needless anxiety.

7.3 Creation or transmission of defamatory material

7.4 Transmission of material which in anyway infringes the copyright of another person

7.5 Transmission of unsolicited commercial advertising material to networks belonging to other organisations

7.6 Deliberate actions or activities with any of the following characteristics:

a. Wasting staff effort or networked resources
b. Corrupting or destroying another users' data
c. Violating the privacy of other users
d. Disrupting the work of other users
e. Other misuse of the networked resources by the deliberate introduction of viruses/malware
f. Playing games during working hours
g. Altering the set up or operating perimeters of any computer equipment without authority.