IT Policy

Introduction

The Council works with IT providers that are appropriate for local government public service compliance. This policy is in the context that all data security and GDPR compliance are adhered to by these providers. All staff and Councillors will be made aware and trained in security and compliance where relevant.

This policy is intended to provide guidance and criteria for Councillors on the use of both the Town Council's email domain addresses, internet and Town Council provided IT equipment whether it be a laptop or tablet (hereon in known as 'device'). Guidance for staff is included in the Employee Handbook.

1. Emails

1.0 Councillors are provided with a Stalham Town Council email address (name of councillor@stalham-tc.gov.uk) and all Town Council correspondence should be sent from this address. Councillors should not use their personal email address in relation to their councillor role.

1.1 Sending offensive emails, such as racist or sexist emails, will never be tolerated and may be subject to report under the Code of Conduct to the Monitoring Officer.

1.2 Dealing with excessive amounts of email can hinder productivity, therefore caution must be exercised. Only relevant emails should be sent, and you should not automatically send or forward all messages to long circulation lists.

1.3 A wrongly delivered message must be redirected correctly and any confidential information contained within such a message must not be used or disclosed.

1.4 Although email communications have the same apparent informality as using the telephone, they also have the permanence of written communications and, as such, care should be taken to ensure that they meet the same standards as other published documents. All communications sent on Town Council email are subject to Freedom of Information disclosure requests.

1.5 Laws which apply to written documents also apply to email and therefore, care must be taken to avoid making inaccurate or defamatory statements. Emails must be composed and sent responsibly, and you should seek advice before sending a message if there is any doubt about its contents.

2. Online Journals, Blogs, YouTube, Facebook, Twitter etc

(Please also refer to the Town Council's Social Media Policy and Media Policy)

2.0 You must never represent your personal views as being those of the Town Council. Please make sure that any personal views expressed are your own.

2.1 If you identify yourself in any way online as being connected with the Town Council, then any online input is indirectly linked to the Town Council. Councillors should therefore have regard to the Code of Conduct.

2.2 The Town Council reserves the right to request you remove or amend any references to the Town Council from all your online posts or comments.

2.3 Similarly, if Town Council confidential information is published online by a Councillor this may be subject to a Code of Conduct complaint.

2.4 On leaving the Town Council for whatsoever reason, you must immediately update any internet profiles to reflect this change.

2.5 These obligations continue without limit in time and may be enforced via the courts if applicable.

3. Data Protection Act

3.0 At all times using email or the internet, you must be fully aware of your responsibilities under the Data Protection Act 2018 and the statutory right of others to request information either by subject access requests or Freedom of Information requests.

4. Back-Up Policy

4.0 The Town Council's IT Network is backed-up daily and this is controlled by Broadland Computers

5. Software

5.0 The software used or developed by the Town Council is confidential and must at no time be used for any purpose other than that for which it is licensed or for which it is authorised to be used by the Town Council, nor removed from the Town Council's premises.

5.1 Viruses, worms and other malicious software (typically introduced through email or infected files) are a significant threat to computer security throughout an organisation. Therefore, every precaution must be taken when using email and/or downloading software.

5.2 You must notify the Town Clerk without delay if your virus protection software notifies you that a virus has been found

5.3 Never load software (this includes illegal or free software) onto any computer belonging to the Town Council without permission of the Town Clerk.

6. Security

6.0 You must adhere to the Town Council's password regulations. You must never provide inappropriate access to Town Council/work-related passwords to any other individual.

6.1 You are also responsible for the security of your allocated device and you must ensure that it is not used by unauthorised people.

6.2 If you are provided with use of a device, it is considered of the utmost importance that you ensure there is appropriate and sufficient security of any sensitive or confidential data.

6.3 Councillors should not download any Town Council or Town Council related data on to any removable storage device without prior agreement with the Town Clerk.

7. Monitoring

7.0 The email system and Internet are available for communications directly concerned with the business of this organisation. The Town Council reserves the right to intercept, monitor and view all data sent or received electronically by you, whether internally or externally, and all Internet sites accessed by you using computer equipment or other property owned by the Town Council. This monitoring would include any information you might consider to be private and personal but has involved the Town Council's IT facilities.

8. Unauthorised use of IT

8.0 Any unauthorised use of email, Internet or the IT systems or breach of this policy may be subject to a Code of Conduct complaint.

8.1 By way of example only, the Town Council will not tolerate the use of the system for any of the following. This list is not exhaustive:

- Accessing, sending and/or downloading offensive, obscene, pornographic or indecent material, or even visiting such websites, is forbidden;
- Posting confidential or derogatory information about employees, the Town Council or its customers or suppliers, whether this is undertaken from the office or on another IT/phone system.
- Any message that could constitute bullying or harassment;
- Accessing, sending and/or downloading discriminatory material or anything that would breach the terms of the equal opportunities policy;
- Downloading or distributing copyright information and/or any other unlicensed software;

9. Ownership and Term of Office (Councillors)

9.0 Councillors are required to use a Town Council owned laptop as part of their tenure as Councillor will be required to complete a Laptop Acceptance Form.

9.1 On resignation of a Councillor, end of term of office or at any point by request of the Town Clerk, the councillor must return any IT equipment, software and related accessories.

9.2 All IT equipment, software, data, related contracts and accessories, provided by the Town Council, remains the property of the Town Council. All data contained on the any IT equipment is the property of the Town Council and the Town Council reserves the right to own, control and interrogate that data

10. Compliance

10.0 All councillors who use Town Council issued IT equipment are obliged to adhere to this policy.

11. Data Protection and Security

11.0 All devices must be encrypted and protected by the Avast business security software. This will be managed centrally by Town Council's IT provider.

11.1 The device will be for Stalham Town Council purposes only. Do not set up your personal email address, or any other email accounts, on this device.

11.2 Do not link up, download or otherwise access personal third-party apps or services, including on-demand TV and other media streaming services.

11.3 You will be required to set a password to access the device. You will receive a prompt periodically to change their password, in line with the Town Council's security measures via the IT provider.

11.4 The password must be unique and must not be recorded. If a password is forgotten please contact a member of staff.

11.5 You must not jailbreak your device (modify or remove restrictions to allow access to restricted sites or the downloading of prohibited software), or otherwise hack or tamper with it.

12. Lost, damaged or stolen devices

12.0 If your device is lost or has been stolen, report it to a member of staff immediately.

12.1 If your device has become damaged, report it to a member of staff and hand the device in to the office.

12.2 You must not carry out repairs to your device.

12.3 You must not solicit any individual or company to repair your device on your behalf.

Revisions	
Date	**Amendment**