Godalming
Town Council
Supporting Our Community

POLICY ON THE ACCEPTABLE USE OF IT FACILITIES

This policy should be read in conjunction with the linked policies listed below:

- Code of Conduct
- Disciplinary Procedure & Rules
- Equality & Diversity Policy
- Data Protection Policy
- Social Media Policy

1. INTRODUCTION

Godalming Town Council's (the Council) information and communication technology systems are used as a tool for managing and delivering the Council's services. Electronic communications play an essential role in the way the Council communicates. All communications from the Council not only reflect on staff members as individuals but also on the Council as an organisation.

The internet assists staff to do their jobs and access information. This policy is designed to help staff understand the Council's expectations for the use of Council resources and to ensure staff use those resources wisely.

This policy seeks to ensure that:

- The Council benefits from technologies whilst maintaining security and legality, avoiding abuse of the systems and protecting the good name of the Council.
- The Council set clear standards of behaviour and conduct in the use of IT.

The communications and IT equipment refers to, but it is not limited to, computers, internet access, remote access connections, email servicers, file storage, webmail, personal digital assistants (iPhones, iPads, Smart-Phones etc.,) telephones, mobile phones and computing and networking facilities owned and operated by the Council.

2. POLICY OVERVIEW

Information and communication technology systems provide a means for communicating both internally and externally and a means for storing information, including personal or sensitive information. All staff and other users are therefore expected to use the systems provided in ways which:

i. Comply with the law (e.g. data protection, equality legislation, health and safety);
ii. Enhance efficiency and productivity; and
iii. Protect the reputation of the Council.

Users must not misuse IT facilities by taking any action which would bring the Council into disrepute, cause offence, interfere with the Council's work or jeopardise the security of data, networks, equipment or software.

The facilities are provided for appropriate Council business. Personal use of IT facilities may be subject to appropriate monitoring. The Council expects all employees to adhere to this policy and is a condition for using the Council's equipment and networks.

The guiding principle is that, despite its immediacy and ease of distribution, electronic communication and information should be treated no differently from that on paper.

3. APPLICABILITY

The policy applies to:-

- All Council full time, part time, casually employed, or temporary employees engaged in work for the Council, including working from home or non-Council locations.
- Other persons working for the Council, whilst engaged on Council business or using Council equipment and networks, including agency workers.

4. PEOPLE RESPONSIBLE FOR IMPLEMENTING THE POLICY

The Town Clerk has overall responsibility for the effective operation of this policy. Responsibility for monitoring and reviewing the operation of this policy and making recommendations for change to minimise risks also lies with the Town Clerk.

Any misuse of the IT resources should be reported to the Town Clerk.

5. COMPLIANCE WITH RELATED POLICIES AND AGREEMENTS

Godalming Town Council's policies and procedures e.g. Codes of Conduct, Disciplinary, and Equality and Diversity apply equally to behaviour online as offline. The IT resources should never be used in a way that breaches any of its other policies.

It is the responsibility of each individual to ensure that information and data that they hold on the Council's computer system fully comply with the principles of the data protection regulations. In brief, the protection of data requires that anyone who inputs, stores, or uses personal information must ensure that the information e.g. names, addresses, other information kept on individuals, is:

- Accurate and up to date;
- Only kept for legitimate purposes;
- Only kept for as long as required;
- Only used for legitimate purposes;
- Not passed on to third parties without the consent of the individual and
- Kept secure.

6. MONITORING

The content of the Council's IT resources and communications systems are the property of the Council. Therefore, staff should have no expectation of privacy in any message, files, data, document, facsimile, telephone conversation, social media post conversation or message, or any other kind of information or communications transmitted to, received or printed from, stored or recorded on the Council's IT and communications systems.

The Council reserves the right to monitor, intercept and review, without further notice, staff's use of the Council's IT resources and communications systems, including but not limited to emails, social media postings and activities, to ensure that its rules are being complied with and for legitimate business purposes. Staff consent to such monitoring by their acknowledgement of this policy and their use of such resources and systems. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings, and other uses of the systems as well as keystroke capturing and other networking monitoring technologies.

The Council may store copies of such data or communications for a period of time after they are created, and may delete such copies from time to time without notice.

Employees should not use the Council's IT resources and communications systems for any matter that they wish to be kept private or confidential from the Council.

The Council exercises the right to intercept emails and internet access under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 for the following reasons:

- To investigate or detect the unauthorised use of the systems,
- To maintain an adequate level of security for its computer systems;
- To detect any computer viruses; and,
- To check mailboxes of absent employees.

To exercise the Council's right under the Regulations, Godalming Town Council must have made all reasonable efforts to inform every person who may use the system that interception may take place. The Council believe that the communication of this policy to all employees meets this requirement.

7. PASSWORDS

- All systems require an authenticated User ID/password combination prior to gaining access.
- Staff should change their password as required by the Council and if they believe their password has been compromised.
- Staff should keep their login details secure.
- A record of all logins, login IDs and passwords for all systems is to be maintained by the Support Services Executive to allow for business continuity. This record is to be maintained in a manuscript format and kept securely.
- It is the responsibility of all staff members to ensure that the Support Services Executive is kept informed of any changes or the creation of any new logins, login IDs or passwords.
- In order to protect information, appropriate passwords on sensitive or confidential data must be set and not disclosed to others except for the point noted above. Responsibility for the security of an individual staff member's password lies with the individual and they should not divulge it to anyone without the Town Clerk's express permission except as indicated above for business continuity purposes.
- Should any staff believe that a login, login ID or password is compromised, they should change it immediately and notify the Support Services Executive and Town Clerk who will take any appropriate further action to maintain the security of the system and the data contained therein.
- Any confidential documents should be encrypted prior to sending via e-mail – the password should be notified separately to the receiver.

8. COMPUTER USAGE

- Computers should be fully shut down and turned off at the end of each day. This includes turning off the screens.
- To prevent unauthorised access to files by third parties eg. members of the public, staff should take appropriate actions/precautions to ensure that data is not accessible by members of the public.
- The computer systems are backed up regularly, however, staff must ensure their work is adequately saved in a secure location that is accessible for backup; desktops and local drives are not backed up.

9. MOBILE PHONE TEXTING

- Texting should be avoided wherever possible. Text messages are the same as any other communication. They must not be illegal, discriminatory, obscene, pornographic or otherwise abusive or threatening messages.

10. APPROPRIATE USE AND MISUSE

10.1 Misuse of Internet and E-Mail

Misuse includes using electronic media for:-

- Creation, use, transmission or encouragement of material that breaches any existing law.
- Transmission of unsolicited commercial or advertising material.
- Obtaining unauthorised access to the Council's or another organisation's IT facilities.
- Violating the privacy of other people.
- Excessive personal use of the internet.
- Deliberately disrupting other users' work in any way, including by viruses or data corruption.
- Expressing personal views, which could be misinterpreted as those of the Council.
- Committing the Council to purchasing or acquiring goods or services without proper authorisation.
- Downloading copyrighted or confidential information, unless authorised. Downloading confidential and/or personal data from the Council's systems without the express permission of the Town Clerk is forbidden.
- Attempting to circumvent by any means the computer or network security.
- Attempting to discover another person's username and password, by any means.
- Installing any software by whatever medium (e.g. data sticks, data transfer) not virus checked and approved by the Council's IT providers.
- Using the computer systems for any activity not related to your work for the Council for personal financial gain.
- Failing to adhere to this policy.

This is not an exhaustive list, but is an indication of the types of conduct that may result in disciplinary action and possible dismissal.

10.2 Offensive and Illegal Material

a. Offensive material is anything, which is pornographic; involves threats or violence; promotes illegal acts, racial or religious hatred or discrimination of any kind. It also covers the use of material that is not in itself explicitly offensive, in a reckless manner such that it causes offence to a colleague.

b. Use of the Council's facilities for accessing offensive material will be considered as gross misconduct.

c. If illegal material is accessed, the Council will inform the Police and criminal prosecution may follow.

d. Accidental access to undesirable web sites should not be a disciplinary matter. Such accidental access should be reported to the Town Clerk. Failure to report accidental access may be considered as a disciplinary matter.

e. People receiving offensive or sexually explicit mail should not forward it to any person but should inform the Town Clerk immediately. Such material may not be identifiable until an E-Mail is opened and in these cases, staff will not be held responsible provided they report it immediately.

f. It is not permitted for any user of the Council's IT facilities to subscribe to inappropriate online services or subscription internet sites.

10.3 Private Use of Facilities

a. Staff may use their Internet connections for occasional private purposes provided that:

- The use is reasonable;
- It does not interfere with Council work;

- It is not related to a personal business use;
- It is not used for commercial purposes, including sale or purchase of goods and services;
- It complies with this policy, including its provisions regarding misuse.

b. The Town Clerk is responsible for monitoring time spent in personal use and if deemed necessary may take appropriate action if required.

10.4 E-Mail

a. E-Mail should be regarded as public and permanent. It is never completely confidential or secure and, despite its apparent temporary nature, it can be stored, re-sent and distributed to large numbers of people.

b. Sending an E-Mail is the same as sending a letter or publishing a document in law, so defamatory comments could result in legal action.

c. It is easy to be misunderstood in E-Mail. People often treat it like telephone calls, but forget that the emotional meaning is often lost in text. Humour can be misinterpreted. E-Mail should be unambiguous.

d. Careful consideration should be given to using bulk E-Mail to external individuals and organisations.

e. Junk mail ("spam") is a hazard of Internet life. Staff should use the Panda security system to block notified spam.

f. All external E-Mails must contain the Council's standard confidentiality clause.

11. INTERNET

11.1 Connections

All connections to the Internet, with the exception of those otherwise authorised, must be via the network to ensure that maximum control and protection is achieved.

11.2 Access

Staff may only join newsgroups or electronically register with other organisations where they relate to professional or Council interest. If in any doubt, staff are to refer to the Town Clerk.

11.3 Virus Protection

a. Viruses can be transferred by files and E-Mail attachments and thereby threaten the security of the Council's network. E-Mail attachments should not be opened unless the E-Mail is from a known source and the covering E-Mail refers to the attachment. If in any doubt staff should delete the email.

b. If staff believe that their system has been or may be infected by a virus they should immediately notify the Council's IT provider.

c. Virus protection software is installed onto each PC. It must not be disabled and the settings must not be altered in any way.

11.4 Software

a. All licensing requirements, payment conditions and deletion dates associated with software must be met.

b. Any software identified as causing problems to the functioning of a PC or the Council's network must be reported to the Council's IT provider.

c. Appropriate screensavers may be used.

d. All installation of software is to be conducted by the Council's IT provider.

12. PUBLICATION ON THE INTERNET

a. The Council's website and its network, are important parts of its external and internal communications. Staff are encouraged to contribute material to both and to seek innovative ways of using them to improve services and consultation.

b. The Council's policy is to operate a single public website.

c. The style and design of the public website is directed by Council policy. All providers of information must adhere to these standards.

d. New material published on the Council website is subject to review and approval by the Town Clerk, who will resolve any queries.

e. Each item of information should have its provider and date of publication identified.

f. Anyone publishing material must not infringe another person's or organisation's copyright and permission must be obtained before using images, text or other material not produced by the Council.

g. If links are desired between the Council's website and those of other organisations the link may only be made by the Support Services Executive. The site to be linked to will be contacted, as a courtesy, to make sure the Council is informed if the site address later changes.

h. The Council owns the copyright to all of its own material. Anyone finding misuse of Godalming material, or its corporate identity on the Internet, should inform the Town Clerk.

13. DISCIPLINARY ACTION OVER SOCIAL MEDIA USE

Failure to follow this policy is a serious disciplinary offence, which could lead to dismissal. Disciplinary action may be taken regardless of whether or not the breach is committed during working hours and regardless of whether or not the Council's equipment or facilities are used for the purpose of committing the breach. Any staff member suspected of committing a breach of this policy will be required to co-operate with the Council's investigation, which may involve handing over relevant passwords and login details. It could also lead to criminal or civil action if illegal material is involved or if legislation, for example the Data Protection Act 1998 or General Data Protection Regulations 2018 are contravened.

This is a non-contractual policy which will be reviewed from time to time.