



BIGGLESWADE TOWN COUNCIL

Internet Acceptable Usage Policy

This document will be distributed to:

Name

Job Title

Email Address

Contents

1. Policy Statement
2. Purpose
3. Scope
4. Definition
5. Risks
6. Applying the Policy
 - 6.1. What is the purpose of providing the Internet service?
 - 6.2. What you should use your Council Internet account for
 - 6.3. Personal use of the Council's Internet service
 - 6.4. Use of Social media
 - 6.5. Internet account management, security and monitoring
 - 6.6. Things you must not do
 - 6.7. Your responsibilities
 - 6.8. Line Manager's responsibilities
 - 6.9. Who should I ask if I have any questions?
 - 6.10. Acceptable Usage Policy
7. Policy Compliance
8. Policy Governance
9. Review and Revision

1. Policy Statement

Biggleswade Town Council will ensure all users of Council provided internet facilities are aware of the acceptable use of such facilities.

2. Purpose

This policy document tells you how you should use your Council Internet facility. It outlines your personal responsibilities and informs what you must and must not do.

The Internet facility is made available for the business purposes of the Council. A certain amount of personal use is permitted in accordance with the statements contained within this Policy.

It is recognised that it is impossible to define precise rules covering all Internet activities available and adherence should be undertaken within the spirit of the policy to ensure productive use of the facility is made.

3. Scope

This Internet Acceptable Usage Policy applies to, but is not limited to, all Biggleswade Town Council Members, Committees, Services, Partners, Employees of the Council, contractual third parties and agents of the Council who access the Council's Internet service and IT equipment.

4. Definition

This Internet Acceptable Usage Policy should be applied at all times whenever using the Council provided Internet facility. This includes access via any access device including a desktop computer, council laptop, or a smartphone device.

5. Risks

Biggleswade Town Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business.

This policy aims to mitigate the following risks:

- Viruses, malware etc.
- Increased risk of data loss and corresponding fines.
- Inappropriate access to and unacceptable use of the Council's network, software, facilities and documents.
- Inadequate destruction of data.
- The non-reporting of information security incidents.
- Inconsistency in how users deal with 'secure' documents.
- The impact of insufficient training for users.
- The sharing of passwords.
- Incorrect or inappropriate classification of documents.
- Risk of reputation damage and further loss in public confidence.
- Operational difficulties providing services.
- Inappropriate sharing of personal data in breach of the Data Protection Act 1998.

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

6. Applying the Policy

6.1. What is the purpose of providing the Internet service?

The Internet service is primarily provided to give Council employees and Members:

- Access to information that is pertinent to fulfilling the Council's business obligations.
- The capability to post updates to Council owned and/or maintained web sites.
- An electronic commerce facility.
- An ability to engage online with our customers.

6.2. What you should use your Council Internet account for

Your Council Internet account should be used in accordance with this policy to access anything in pursuance of your work including:

- Access to and/or provision of information.
- Research.
- Accessing browser based IT applications.

6.3. Personal use of the Council's Internet service

At the discretion of your line manager, and provided it does not interfere with your work, the Council permits the use of the Internet facilities for non-business research or browsing during unpaid meal-times or unpaid before/after flexi-time/normal working hours.

Personal use of the Internet is subject to management discretion and the following conditions:

- To investigate or detect the unauthorised use of the systems, e.g. that the policy is being observed, that no discriminatory or offensive content appears in emails, etc.
- That personal use does not impinge on the member of staff's work or that of other staff;
- That personal use takes place outside of normal working hours and that the time is not included in the calculation of daily hours; and
- That personal use is not connected to any business or profit making venture. In addition to these general restrictions noted above, the Council specifically excludes the following uses of the Internet:
 - To view content of an obscene or discriminatory nature, or content that is in violation of UK legislation.
 - To download unofficial software for use on Council equipment.
 - To reveal confidential information.
 - To spread or publish any political, with the exception of recognised Trade Union Activity, or threatening views or content that could cause unrest. To search for personal information using the business email address.

6.4. Use of Social media

- You must not access social networking sites for personal use during working hours. Access to the Web using the Councils IT systems is restricted to lunch breaks and before and after the working day, unless specific permission is granted by your manager.
- You may not use Facebook page for personal blogs.
- Employees must not give information on a social networking site which is confidential to the Council, its suppliers or customers.
- Employees must refrain from making reference on social networking sites to the Council, its employees, its customers and its suppliers.
- Employees must not post entries on Facebook or a social networking site which are derogatory, defamatory, discriminatory or offensive in any way, or which could bring the Council into disrepute.
- Employees should be aware that blogs may create documents which the courts can order to be disclosed for use in litigation. Consequently, employees will be assumed to have written any contentious items unless they can prove definitively that they have not done so.
- The Council will monitor its IT systems as is deemed necessary in order to prevent inappropriate usage Monitoring use of social media during work time.
- The Council reserves the right to monitor employees Internet usage, the Council considers that valid reasons for checking and employees Internet usage include suspicions that the employee has:

been spending an excessive amount of time using social media websites for non-work-related activity; or
acted in a way that is in breach of the rules set out in this policy
- The Council reserves the right to retain information that it has gathered on employees use of the Internet for a period of one year.
- Access to particular social media sites may be withdrawn in any case of misuse.

Note:

Access to on-line games and the use of social chat rooms or forums will be reviewed and may be blocked for business reasons e.g. streaming media, impact on services, or due to content being downloaded.

Staff purchase personal items at their own risk. The Council is not responsible for any personal transactions you enter into. You must accept responsibility for, and keep the Council protected against, any claims, damages, losses or the like which might arise from your transaction – for example in relation to payment for the items or any personal injury or damage to property they might cause.

If you are in any doubt about how you may make personal use of the Council's Internet service, you are advised to discuss this with your Manager.

All personal usage must be in accordance with this policy. Your computer and any data held on it are the property of Biggleswade Town Council and may be accessed at any time by the Council to ensure compliance with all its statutory, regulatory and internal policy requirements.

6.5. Internet account management, security and monitoring

The Council will provide a secure logon-id and password facility for the network which will include access to the internet. The Council's outsourced IT provider is responsible for the technical management of this account.

The provision of Internet access is owned by the Council and all access is recorded, logged and interrogated for the purposes of:

- Monitoring total usage to ensure business use is not impacted by lack of capacity.
- The filtering system monitors and records all access for reports that are produced for line managers and auditors.

6.6. Things you must not do

Access to the following categories of websites is currently blocked using the Websense URL filtering system.

Please note that this is not exhaustive and will be updated as appropriate:

- Illegal.
- Pornographic.
- Violence.
- Hate and discrimination.
- Offensive.
- Weapons.
- Hacking.
- Gambling.
- Dating.
- Radio stations.
- Games.

Except where it is strictly and necessarily required for your work, for example IT audit activity or other investigation, you must not use your Internet account to:

Create, download, upload, display or access knowingly, sites that contain pornography or other "unsuitable" material that might be deemed illegal, obscene or offensive.

Subscribe to, enter or use peer-to-peer networks or install software that allows sharing of music, video or image files.

Subscribe to, enter or utilise real time chat facilities such as chat rooms, text messenger or pager programs.

Subscribe to, enter or use online gaming or betting sites.

Subscribe to or enter “money making” sites or enter or use “money making” programs.

Run a private business.

Download any software that does not comply with the Council’s Software Policy. The above list gives examples of “unsuitable” usage but is neither exclusive nor exhaustive. “Unsuitable” material would include data, images, audio files or video files the transmission of which is illegal under British law, and, material that is against the rules, essence and spirit of this and other Council policies.

6.7. Your responsibilities

It is your responsibility to:

Familiarise yourself with the detail, essence and spirit of this policy before using the Internet facility provided for your work.

Assess any risks associated with Internet usage and ensure that the Internet is the most appropriate mechanism to use.

Know that you may only use the Council’s Internet facility within the terms described herein.

Read and abide by the following related policies: Email Acceptable Use Policy. Software Policy.IT Access Policy. Removable Media Policy.

6.8. Line Manager’s responsibilities

It is the responsibility of Line Managers to ensure that the use of the Internet facility:

Within an employees work time is relevant to and appropriate to the Council’s business and within the context of the user’s responsibilities.

Within an employee’s own time is subject to the rules contained within this document.

6.9. Who should I ask if I have any questions?

You should refer questions about this policy to your Line Manager.

You should refer technical queries about the Council’s Internet service to the outsourced IT provider’s.

6.10. Acceptable Usage Policy

Each user must read, understand and sign to verify they have read and accepted this policy.

This policy must be signed annually.

- I understand and agree to comply with the Internet Acceptable Usage Policy of my organisation.

Signature of User:

.....

A copy of this agreement is to be retained by the User and Employee Services.

Document Date: [Date signed and agreed by staff member]

Name of User: [Surname, First Name]

Job Title: [Job Title]

7. Policy Compliance

If any user is found to have breached this policy, they will be subject to Biggleswade Town Council's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from Business Systems.

8. Policy Governance

The following table identifies who within Biggleswade Town Council is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- Responsible – the person(s) responsible for developing and implementing the policy.
- Accountable – the person who has ultimate accountability and authority for the policy.
- Consulted – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- Informed – the person(s) or groups to be informed after policy implementation or amendment.

Responsible

Town Council and Committees.

Accountable

Town Clerk

Consulted

The Councillors and Committee members.

Informed

All Council Employees, All Temporary Staff, All Contractors.

9. Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.