# Bromsgrove District Council

# Members ICT Policy

# July 2021

**Table of Contents**

## 1 Policy Statement

Bromsgrove Council Members require access to information that enables them to perform their duties as a councillor. Much of this information can be provided electronically via email, word processing and spreadsheet files. The Council's general presumption is for electronic provision of information / transaction of business.

## 2 Purpose

The purpose of this policy is to ensure that Bromsgrove District Councillors can access Information and Communication Technology (ICT) facilities whilst maintaining compliance with Central Government's Public Service Network (PSN) and other related policies.

The Council holds large amounts of personal and restricted information. Information security is very important to help protect the interests and confidentiality of the Council and its customers. Information security cannot be achieved by technical means alone. Information security must also be enforced and applied by the people who use it and those who provide support for it.

## 3 Scope

This policy applies to any Councillor that requires access to Council information systems such as email or other documents, whether it is a temporary or permanent arrangement.

## 4 Definition

The Council understands that to reduce the risk of theft, fraud or inappropriate use of its information systems, anyone that is given access to Council information systems **must**:

- Be suitable for their roles.
- Fully understand their responsibilities for ensuring the security of the information.
- Only have access to the information they need.
- Request that this access be removed as soon as it is no longer required.
- Complete Data Protection training to ensure Members are clear on how information can be used when they are working on behalf of the council and when they are working on behalf of constituents, and how it should be stored.
- Ensure that no personal information that could be in breach of the data protection act, is stored on their laptop or other unencrypted device.

This policy must therefore be applied prior, during and after any user's access to information or information systems used to deliver Council business.

## 5 Provision for ICT equipment.

The Council recognises that individual Councillors have a requirement to access electronic information.

The governments zero tolerance approach to compliance with the PSN code of connection, has required the implementation of innovative methods of accessing ICT, whilst remaining within the budget and resource limitations of the Authority. Should the limits of the budget be reached, the Leader of the Council will revisit current ICT needs for the future.

The council will not automatically forward Council emails to personal email accounts such as Hotmail, Google mail etc. This is to ensure the authority complies with the Government's PSN code of connection.

**Option One**

The Authority will provide either a standard Laptop or a lighter, more portable, touch screen MS Surface Pro device. This will enable the Councillor to access the internet, corporate emails, corporate calendars, Microsoft Teams, Modern.Gov, MS Office suite and necessary documents. This option will include a security practice known as two factor authentication (2FA). This provides an additional security step using either a mobile phone or a physical token device. Members can choose which of these 2FA methods they wish to use and a token device will be provided if a mobile phone is either not available or not preferred.

Additional security may be added at a future date to keep in line with new PSN policy requirements.

Broadband services are to be provided by the Councillor and expenses for these claimed through the normal expenditure claim process at £100 per year (maximum 1 per household).

Support for the Laptop or Surface Pro Device will be provided by the authority's ICT department by telephoning 01527 881766 Mon-Fri 8:30 to 17:00.

All internet usage and electronic communication – including but not limited to emails and chat, sent and received via the corporate device, will be subject to automated scanning, monitoring and filtering to assist with ICT security and adherence to additional policies as described in section 9. This information can also be used to ensure relevant laws are adhered to.

Emails and Chat messages are automatically erased on a rolling 2 year basis but Members are requested to delete all information as soon as it becomes no longer needed.

It is the Councillor's responsibility to ensure their password for accessing any Corporate Information service is not shared with any other person and that connection to such services is ended by logging off the system, as soon as work is completed or the connection is left unattended. This is to prevent unauthorised access to information.

If it suspected that someone else may know their password, or any security problem has occurred, Councillors must report this to the helpdesk immediately so it can be rectified.

Insurance for equipment provided by the council, is provided by the Authority but Members are asked to ensure they store the device securely and take any appropriate measures to protect the device whilst in use. Insurance claims made will incur a £100 excess charge to the Democratic Services department

The Council provides the Laptop or Surface Pro device together with ancillary equipment and materials required, for the Councillor's functions as a Councillor. Use of this equipment for any other reason, including personal use or use by anyone other than a Councillor is not permitted.

All ICT equipment provided by the authority remains the property of the Council and must be returned at the end of the election term.

**Option Two (can be in addition to Option One)**

The Councillor provides their own Microsoft Laptop, Android or Apple device and the council provides technically secure software to enable the Councillor to access the internet, corporate emails, corporate calendars, Microsoft Teams, Modern.Gov, MS Office suite and necessary documents. This option will include a security practice known as two factor authentication (2FA). This provides an additional security step using either a mobile phone or a physical token device. Members can choose which of these 2FA methods they wish to use and a token device will be provided if a mobile phone is either not available or not preferred. The same 2FA ca be used as per option1 if this option has already been selected.

Additional security may be added at a future date to keep in line with new PSN policy requirements.

Broadband services are to be provided by the Councillor and expenses for these claimed through the normal expenditure claim process at £100 per year (maximum 1 per household).

Support for the Councils Software, but not the device it is installed on, will be provided by the authority's ICT department by telephoning 01527 881766 Mon-Fri 8:30 to 17:00.

All internet usage and electronic communication sent via the councils login credentials – including but not limited to emails and chat, both sent and received, will be subject to automated scanning, monitoring and filtering to assist with ICT security and adherence to additional policies as described in section 9. This information can also be used to ensure relevant laws are adhered to.

It is the Councillor's responsibility to ensure their password for accessing any Corporate Information service is not shared with any other person and that connection to such services is ended by logging off the system, as soon as work is completed or the connection is left unattended. This is to prevent unauthorised access to information.

If it suspected that someone else may know their password, or any security problem has occurred, Councillors must report this to the helpdesk immediately so it can be rectified.

All ICT equipment (including software licenses) provided by the authority remains the property of the Council and must be returned at the end of the election term.

## 6 Policy Compliance

If any Member is found to have breached this policy, IT provision will be withdrawn. 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, please seek advice from Members' Services or ICT.

## 7 Policy Governance

The following table identifies who within the 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** | ICT Transformation Manager |
| **Accountable** | Head of Transformation, Organisational Development & Digital Services |
| **Consulted** | Corporate Management Team, Members' Services |
| **Informed** | All Councillors |

## 8 Review and Revision

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

Policy review will be undertaken by the ICT Transformation Manager.

## 9 References

The following Bromsgrove District Council policy documents are directly relevant to this policy.

- Central Government's PSN Policy
- Information Security Policy.
- Members' Code of Conduct and related Codes and Protocols.
- Social Media Policy.

## 10 Receipt and acceptance statement

I, Councillor _____ agree to comply with the policy items as stated within this document.

Signed _____ Date _____

PLEASE RETURN COMPLETED STATEMENT AS SOON AS POSSIBLE TO :

Democtractic Services
Bromsgrove District Council
Parkside