WESTBURY-ON-SEVERN PARISH COUNCIL

REMOTE ACCESS POLICY

Remote Access refers to any technology that enables you to connect users in geographically dispersed locations. This access is typically over some kind of dial-up or internet connection.

1. Purpose of Policy

Remote access by Westbury-on-Severn Councillors and staff is a method of accessing files and systems remotely. In practice, the benefits of securing remote access are considerable. Westbury-on-Severn Parish Council (WoSPC) business can be conducted remotely with confidence and confidentiality. This document sets out the policy for remote access and includes a set of common controls, which WoSPC applies to reduce the risks associated with a remote access service.

2. Scope

This policy covers all types of remote access, whether fixed or 'roving' including:

2.1. Councillors and staff away from their normal location
2.2. Councillors and staff at their homes
2.3. Contractors and other 3rd party organisations
2.4. The general public.

3. Objectives

The objectives of the remote access by Councillors and staff are:

3.1. To provide secure and resilient remote access to WoSPC's information and systems.
3.2. To preserve the integrity, availability and confidentiality of WoSPC's information and information systems.
3.3. To manage the risk of serious financial loss, loss of client confidence or other serious impact which may result from a failure in security.
3.4. To comply with all relevant regulatory and legislative requirements (including General Data Protection Regulations) and to ensure that the Council is adequately protected under computer misuse legislation.

4. Principles

In provision of remote access, the following high-level principles will be applied:

4.1. Councillors will appoint to have overall responsibility for each remote access connection to ensure that the Council's policy and standards controlled.
4.2. A formal risk analysis process will be conducted for each application to which remote access is granted to assess risks and identify controls needed to reduce risks to an acceptable level.
4.3. Remote users will be restricted to the appropriate services and functions necessary to carry out their role.

5. Responsibilities

5.1. WoSPC is ultimately responsible for ensuring that remote access by staff is managed securely.
5.2. WoSPC will maintain policy, standards and procedures for remote access to ensure that risks are identified and appropriate controls implemented to reduce those risks.
5.3. WoSPC takes responsible for confirming whether remote access to business applications and systems is permitted.
5.4. Councillors and staff will ensure that their user profiles and logical access controls are implemented in accordance with agreed access levels.
5.5. Assistance on implementing controls will be provided where needed.
5.6. All remote access users are responsible for complying with this policy and associated standards. They must safeguard corporate and/or their own equipment and information resources and notify the Clerk immediately of any actual or suspected security incidents and breaches.
5.7. Users must return all relevant WoSPC owned remote access equipment on termination of the need.

6. Risks

WoSPC recognises that by providing Councillors and staff with remote access to information systems, risks are introduced that may result in serious business impact, for example:

6.1. unavailability of systems or target information
6.2. degraded performance of remote connections
6.3. loss or corruption of sensitive data
6.4. breach of confidentiality
6.5. loss of or damage to equipment
6.6. breach of legislation or non-compliance with regulatory or ethical standards.

7. Security Architecture

The security architecture employed by Councillors and staff shall include:

7.1. Strong computer/smart phones/tablets start-up passwords
7.2. Strong service password authentications, authorisation, and accounting
7.3. Security monitoring by intrusion detection systems (*e.g.* firewalls and antivirus/security software/hardware)

8. Security Technologies

To ensure the most comprehensive level of protection possible, security architecture used must include:

8.1. User Identity

All remote users must be registered and authorised. User identity must include and be capable of confirmation that their facilities use strong authentication User ID and password authentication. All Councillors and staff are responsible to WoSPC for this. Failure could lead to implications

8.2. Secure Connectivity

WoSPC will protect confidential information from eavesdropping or tampering during transmission and only make it available on a need to know basis.

8.3. Security Monitoring

WoSPC will make use of appropriate external resource to identify areas of weakness, and monitor suspected security breaches and reactively respond to security events as they occur.

8.4. Remote diagnostic services and 3rd parties

8.4.1. WoSPC accepts that suppliers of central systems/software expect to have dial up access to such systems on request to investigate/fix faults. WoSPC's Councillors and staff will permit such access subject to it being initiated by the computer system and all activity monitored.

8.4.2. All Councillors, staff, contractors, 3rd parties and general public using remote access will be required to commit to maintaining confidentiality of data and information.

8.5. User Responsibilities, Awareness & Training

WoSPC Practice will ensure that all users of information systems, applications and the networks are provided with the necessary security guidance, awareness and where appropriate training to discharge their security responsibilities.

9. Reporting Security Incidents & Weaknesses

All suspected security weaknesses and incidents must be reported to the Clerk**.**

10. Guidelines and training

Access to written guidance and training materials for all remote access users will be made available.

11. Validity of this Policy

This policy will be subject to review in the light of changes to legisation or then current advice. Associated information security standards should be subject to an on going development and review programme.