ICT Remote Access Policy

1. Introduction

1.1. The purpose of this policy is to ensure that security of information and systems when accessed through remote access and/or mobile devices is given due importance. It is essential that staff have the knowledge that security procedures and policies exist and they are understood and adhered to.

1.2. Working from home, whilst travelling, at a client's site or at any other location away from the established (physical) office may be attractive and offer benefits. However, opening up the Council's information and systems through remote access and mobile working also presents security risks. Intruders (hackers, electronic eavesdroppers, shoulder surfers etc) may be able to access, read and potentially modify the Council's information and systems without having to be on site.

1.3. This policy defines how the remote access and mobile working methods should be used to access the Council's data in a secure manner.

1.4. The ICT Department also recognises the unique challenges of connectivity on the Isles of Scilly. Access to the Councils network is limited by the speed of the internet available on the Islands.

2. Scope

2.1. The policy covers everyone who accesses the Council's data from a remote location or with a mobile device. Specifically, Council employees on permanent, temporary and fixed term contracts, temporary or casual staff, volunteers, contractors and other staff employed by a third party and who use Council's facilities.

2.2. Devices that can be used for remote access or mobile working may include equipment such as laptops, notebooks, tablets, smart phones, mobile phones, digital cameras etc

2.3. Information that is related to and can identify an individual is personal data and protected by the principles of the Data Protection Act. As such the appropriate technical and organisational measures shall be taken against accidental or deliberate loss, change, destruction of, or damage to personal data. This policy has been produced to ensure that protection of personal data is maintained whilst accessing data or applications remotely or from a mobile device.

3. Sources of Help

3.1. The ICT Service desk provides a single point of contact for all staff with any operational problem or service request.

4. Access to Systems

4.1. Access to the Council's information, applications (including email) and data can be obtained via the secure Juniper access portal (https://remote.scilly.gov.uk). Access to this portal requires two factors of authentication – a username and password, and a SMS code which will be sent to a nominated mobile phone

4.2. Non council owned PC's and devices will not be able to connect to the Council's network unless they have been examined by the ICT Helpdesk. The ICT Helpdesk will assess the health of the home pc and make recommendations as to whether it can access the Council's network.

4.3. All attempts (failed and unsuccessful) to log into the access portal are logged.

4.4. File transfers to the local PC will generally not be allowed

4.5. Sensitive data should not be printed.

4.6. However where the above usage is unavoidable, an email from an appropriate Line Manger will be sent to the ICT Helpdesk to request these facilities to be activated. The responsibility for the security and integrity of the copied data will then be passed on to the user. Printed material should be disposed of in a secure manner after use (e.g. shredding).

4.7. Applications containing personally identifiable data should not be used in or accessed from public places (eg airports, trains etc). There is no access to the GCSx network remotely.

4.8. Staff should try to access the internet via a cabled connection. If staff have to use Wi-Fi, then the connection should have a minimum encryption standard of WPA2

4.9. All users accessing the council's networks via remote access and mobile devices must abide by the Council's associated security policies and any applicable codes of connection and conduct.

4.10. Employees given devices to enable remote working should not allow or give permission for unauthorised users (including family and friends) to use that device.

4.11. Users of remote access should be aware of the potential for other people (including family, friends, colleagues and intruders) to overlook screens and keyboards and view personal, confidential information or passwords. Users should check this is not taking place.

4.12. Users must not alter or disable any element of the configuration of devices, including data encryption and anti-virus software.

4.13. Only Council provided removable media (eg USB sticks) should be used and must be safely 'closed' if necessary and removed from any device when finished with.

5. Review

This Policy shall be reviewed annually by staff of the ICT Department and submitted for approval to the relevant committee.

Law relating to this document:
Leading Statutory authority: Data Protection Act 1998
Human Rights Act 1998
Regulation of Investigatory Powers Act 2000
Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699)
Employment Practices Data Protection Code (on the Information Commissioner's website)
D Marcus, Feb 2013, ICT Technical Officer