PSPS
Public Sector Partnership Services Ltd

Delivering services for South Holland District Council, Boston Borough Council, East Lindsey District Council

Appendix C

Information Security Policy
Remote Working

May 2021

Document Control

Version Control

Issue Number	Issue Author	Issue Date	Reason for Issue
0.1	J Wright	Mar 18	Initial Draft for review
1.0	J Wright	Sept 18	Revised in readiness for approval
1.1	J Wright	Jan 19	Revised due to comments by PSPS DPO and inclusion of HR elements
1.2	J Wright	Feb 19	Rebrand
2.0	J Wright	Feb 21	Periodic policy review
2.1	J Wright	May 21	Review to include Boston Borough Council

Approval Control

Issue Number	Approval Authority	Name	Approval Date	Due for Review
2.1	SHDC	James Gilbert		
	ELDC/BBC	James Gilbert	May-21	May-24
	PSPS	Lewis Ducket	May-21	May-24

Contents

1. Policy Aim

The aim of this Policy is to define the broad mechanisms and roles through which the Organisation will be able to demonstrate accountability and compliance with regards to the security of the ICT environment for remote workers.

Responsible	Head of ICT & Digital
Accountable	Chief Executive (PSPS), Assistant Director (SHDC/ELDC/BBC)
Consulted	Data Protection Officers, ICT Security Lead
Informed	All Remote ICT Users

2. Introduction

This is a joint Remote Working Policy. Where "The Organisation" is referenced, this refers to either Public Sector Partnership Services or its Client Council's South Holland District Council, East Lindsey District Council or Boston Borough Council.

The purpose of this policy is to define rules and requirements for connecting to the Organisation's network from any host. These rules and requirements are designed to minimize the potential exposure to the Organisation from damages which may result from unauthorised use of resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical internal systems, and fines or other financial liabilities incurred as a result of those losses.

Remote access to our corporate network is essential to maintain productivity, but invariably the very nature of working remotely has inherit risks:

- Increased risk of equipment damage, loss or theft.
- Accidental or deliberate overlooking by unauthorised individuals.
- Unauthorised access to personal or confidential information.
- Unauthorised introduction of malicious software and viruses.

This policy aims to guide and mitigate against such risks.

This policy applies to Councillors, employees, contractors, consultants, temporaries, and other workers at the Organisation, including all personnel affiliated with third parties, who use the Organisation's ICT facilities and equipment remotely, or who

require remote access to the Information Systems or information, including reading or sending email and viewing intranet web resources. This policy covers any and all technical implementations of remote access used to connect to the Organisation's networks.

This policy should be adhered to at all times whenever any user makes use of portable computing devices. This policy applies to all users' use of the Organisation's IT equipment and personal IT equipment when working on official business away from the Organisation's premises (i.e. working remotely).

Portable computing devices include, but are not restricted to, the following:

- Laptop computers
- Tablet PCs
- PDAs
- Mobile phones
- Wireless technologies

This Remote Working Policy forms part of the Information Security Framework.

3. Roles and Responsibilities

The following roles are those formally defined within the Policy:

Role	Responsibility
The Organisation's Chief Executive	Supporting Company/Authority compliance with the policy
Senior Management Team	Ensuring the policy adheres to statutory legislation & guidance and that it is embedded in the workforce and ensuring managers and Team Leaders show compliance with the policy and it is understood.
Managers & Team Leaders	Understanding and complying with the policy, ensuring it is available to team members, and advising on it.
All Staff	Understanding and complying with the policy.

4. Policy Statement

It is the responsibility of the Organisation's Councillors, employees, contractors, vendors and agents with remote access privileges to the corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection.

All ICT equipment (including portable computer devices) supplied to users is the property of the Organisation. It must be returned upon the request.

Only Organisation supplied equipment is to be used for remotely accessing Organisation ICT systems and data.

Third party access to the Organisation's network, primarily software vendors, will have their access restricted to the systems for which they have been contracted to support. Third party connections must comply with the requirements as stated in the Third Party Access Standard.

5.1 User Responsibility

It is the user's responsibility to ensure that the following points are adhered to at all times.

1. All users must comply with appropriate codes and policies associated with the use of ICT equipment.
2. All users must comply with the Employee/Members Access Policy.
3. All users are expected to undertake a Risk Assessment of their working environment in accordance with Health & Safety policies.
4. All users are expected to promptly report the theft, loss or unauthorized disclosure of the Organisation's proprietary information or Equipment, in accordance with Data Protection Policy and the associated Breach Management Procedure.
5. All users are expected to undertake a dynamic risk assessment for their working location, to include, but not limited to, the ability for non Organisation staff to view corporate and potentially sensitive data.
6. All users have a responsibility to promptly report the theft, loss or unauthorized access of the Organisation's equipment in accordance with the ICT Incident Management Procedure, Data Protection Policy and the associated Breach Management Procedure.
7. Users must take due care and attention of portable computer devices when moving between home and another business site.
8. Users will not install any software on to an Organisation owned portable computer device without the prior agreement from ICT.

9. Users will not change the configuration of any Organisation owned portable computer device.
10. Users will not install any hardware on to or inside any Organisation owned portable computer device, unless authorised by a member of the ICT Department.
11. Users will allow the installation and maintenance of Anti-Virus updates immediately.
12. Users will allow the installation of software patches and updates immediately.
13. Users will return the device to Organisation's sites at periodic intervals to allow for the installation of major updates and changes, as deemed necessary by the ICT department.
14. Users will inform the ICT Service Desk of any Organisation owned portable computer device message relating to configuration changes.
15. Any files containing personal data or data which is business critical should be stored on the Organisation's centralised file servers wherever possible and not held on portable computer devices.
16. All faults must be reported to the ICT Service Desk.
17. Users must not deliberately remove or deface any asset registration number.
18. User requests for upgrades of hardware or software must be approved by an authorised member of staff. Equipment and software will then be purchased and installed by a member of the ICT Department.
19. No family members may use the ICT equipment. The ICT equipment is supplied for the staff members' sole use.
20. The user must ensure that reasonable care is taken of the ICT equipment supplied. Where any fault in the equipment has been caused by the user, in breach of the above paragraphs, the Organisation may recover the costs of any repair.
21. The user should seek advice from the Organisation before taking any supplied ICT equipment outside the United Kingdom. The equipment may not be covered by the Organisation's normal insurance against loss or theft and the equipment is liable to be confiscated by Airport Security personnel.
22. The Organisation may at any time, and without notice, request a software and hardware audit, and may be required to remove any equipment at the time of the audit for further inspection. All users must co-operate fully with any such audit
23. Any user who chooses to undertake work at home or remotely in relation to their official duties using their own ICT equipment must understand that they are not permitted to hold any database, or carry out any processing of personal or confidential information relating to the Organisation, its employees, or customers.
24. Under no circumstances should personal or confidential information be emailed to a private non-Organisation email address.

5.2 Remote & Mobile Working Arrangements

Remote or home working should be in line with the Organisation's Flexible or Agile Working Policy and in agreement with the manager.

Agreement should be reached between the manager and colleague as to:

- how the colleague will record their time worked (for example, maintain a timesheet for submission to their manager weekly)
- the frequency of contact required between them – on the phone and in person
- the nature of the contact – management visits, 121's, Team meeting participation etc.
- how often the colleague will be required to attend the office (ideally this should be at least weekly)
- arrangements for attendance at team meetings, staff briefings, etc.

The Organisation retains the right to monitor and access use of its data and systems/services to ensure continued compliance with this policy.

The Organisation retains the right to use a performance/productivity monitoring system to monitor and report on the ICT usage within the Organisation. Use of such a system will undergo required DPIA and DPO approval.

All homeworking arrangements are subject to being removed or amended due to business need or in circumstances where the colleague is not performing to the required standard, without the colleagues' prior consent.

All colleagues should be aware of the physical security dangers and risks associated with working within any remote office or mobile working location.

Equipment should not be left where it would attract the interests of the opportunist thief. In the home it should also be located out of sight of the casual visitor. Devices should not be left either on or in standby mode, with Bluetooth\wireless devices turned on.

For home working it is recommended that the office area of the house should be kept separate from the rest of the house. Equipment must be secured whenever it is not in use.

Users must ensure that access / authentication tokens and personal identification numbers are kept in a separate location to the portable computer device at all times.

All removable media devices and paper documentation must also not be stored with the portable computer device.

Paper documents are vulnerable to theft if left accessible to unauthorised people. These should be securely locked away in suitable facilities (e.g. secure filing cabinets) when not in use. Waste paper containing personal or confidential information must be shredded to required standards.

5.3 Access Controls

It is essential that access to all personal or confidential information is controlled. This can be done through physical controls, such as locking the home office or locking the computer's keyboard. Alternatively, or in addition, this can be done logically such as by password controls or User Login controls.

Portable computer devices should be switched off, logged off, or the keyboard locked when left unattended, even if only for a few minutes.

All data on portable computer devices must, where possible be encrypted. If this is not possible, then all personal or confidential data held on the portable device must be encrypted.

The approved Virtual Private Network (VPN) software or hardware device must be configured to allow remote users access to Organisation's systems if connecting over Public Networks, such as the Internet. This must use or be used upon an approved client provided by the Organisation.

Connecting to cloud based service that hold corporate information should only be conducted from a corporate device; for example MS 365

The corporate device acts as MFA for the user's primary tenant, with a separate MFA token or authenticator app for secondary tenants

Two-factor authentication must be used when accessing the Organisation's network and information systems (including Outlook Web Access) remotely. Such authentication involves the use of "something you have" e.g. a certificate on a laptop or a supplied Remote Access Point and "something you know" e.g. a password.

Employees may be asked to use their own personal smart phone for Two-factor Authentication using Google or Microsoft Authenticator services. The amount of mobile data used for this process is minimal or none if the device is connected to

wireless. This is a reasonable expectation of employees; however alternate means can be provided should it be required.

Access to the Internet from supplied ICT equipment, should only be allowed via onward connection through the Organisation's Proxy Servers and not directly to the Internet.

5.4 Anti-virus Protection

All ICT equipment will have the latest Anti-Virus signature and Windows Update files when connected to the network. Users who work remotely must ensure that their portable computer devices are connected to the corporate network at least daily to enable the Anti-Virus software to be updated.

6 Review

As a standard principle, this policy should be reviewed at least once every two years to ensure that it remains fit for purpose. It may need reviewing more regularly in response to specific legislation changes or changes to best practice guidance.

7 Policy Compliance

If any user is found to have breached this policy, they will be subject to the Organisation'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 the ICT Department.

8 Related Policies

Data Protection Policy

Flexible/Agile Working Policy

Remote/Home Working Policy

Breach Management Procedure

ICT Incident Management Procedure

Acceptable Use Policy

Third Party Access Standard

Employers Code of Conduct

Employers Disciplinary Policy