PS177 Remote Working Policy

January 2014

Version 2.0

Statement of Legislative Compliance

This document has been drafted to comply with the general and specific duties in the Equality Act 2010; Data Protection Act; Freedom of Information Act; European Convention of Human Rights; Employment Act 2002; Employment Relations Act 1999, and other legislation relevant to policing.

Table of Contents

Aims and Objectives of the Policy

This policy aims to establish minimum protective measures by outlining the physical and technical controls applicable when working on official information away from official premises. The policy is designed to provide clear, definitive and unambiguous direction for all those involved in remote working. This should help to protect the Nottinghamshire Police Computer Network, equipment and the information that it holds.

A broad objective is to enable the organisation and its employees to gain the maximum business benefit from using force information.

More specific associated objectives are to:

a) Safeguard the organisation's information.
b) Protect the organisation from potential legal liabilities and protect the reputation of Nottinghamshire Police.
c) Ensure all individuals using force information in remote locations understand their personal responsibilities.
d) Ensure that ICT systems and equipment used for remote working are used appropriately.

Policy Statement

Application and Scope

The policy applies to the use of all Nottinghamshire Police information from any remote working location. Remote workers must ensure that they read, understand and comply with all relevant force policies and those procedures contained within, or referenced from, this document. Failure to comply may lead to a breach in system security and consequently may lead to disciplinary action.

Remote working refers to any work done outside of Nottinghamshire Police premises, including accessing, storing, processing or discussing business information. This could be at home, at another force or at a partner agency.

It also covers mobile working; travelling on public or private transport; staying in hotels; in public places such as libraries or coffee shops or even having telephone conversations in the street. All system use is audited and system users should have no expectation of privacy. Nottinghamshire Police will take criminal and/or disciplinary action against any employee who wilfully misuses its systems.

The Counter Corruption Unit will retain responsibility for ensuring that the use of ICT systems and force information is audited and monitored on an ongoing basis.

Personal Responsibility

All users of Nottinghamshire Police ICT systems, equipment and information have a personal responsibility to protect force information and assets that are under their control. This includes keeping them physically safe when in transit and securely storing all papers and portable ICT equipment when work is finished.

When working from home it is the personal responsibility of the individual to make sure information is safe and the individual’s household understands the need for the security measures to be taken - See PS 164 Homeworking Policy and PD 625Homeworking Procedures

Security Measures

The following points cover the security measures needed to work securely outside of Nottinghamshire Police premises.

It is necessary to:

a) Obtain approval before commencement of remote working.
b) Be familiar with and abide by the security requirements of all force policies and legislation and in particular:

- Acceptable Use Policy & Generic Syops
- GPMS Policy
- Internet & E-mail Policy

c) Have completed an Information Assurance e-learning package within the last 12 months.
d) Consider the GPMS protective marking of the information you will be working on and handle this in line with force policies and procedures.
e) Transport papers, portable ICT equipment, official briefcases, Blackberry devices and mobile phones securely. Keep them with you at all times when travelling and store them securely. Do not leave force information in vehicles that are left unattended i.e. overnight or during breaks in journeys.
f) Make sure your location is sensibly secure to work in, for example it is not overlooked. Do not work on sensitive matters in a public place. If working from home, if possible, use a room where the door can be closed and may be locked at the end of the day.
g) Put your papers away and lock your laptop/PC if stepping away from your ICT equipment.
h) Remember that telephone calls are not a secure method of communication; be aware telephone calls are transmitted over open lines.
i) Ensure that removable media containing force information is encrypted where necessary – this is a mandatory requirement. Do not transfer information from an encrypted device to either an unencrypted or personal device.
j) Always record business information on approved ICT equipment. Be aware that the Freedom of Information Act applies to any information concerning official business, potentially including that which is held in personal email accounts or on your personal ICT equipment.
k) Bring protectively marked information back into the office for secure disposal if there is no approved secure destruction facility available.
l) Contact the Service desk, if travelling or working overseas, to check whether your devices will work and whether any security restrictions apply
m) It is vital that remote workers **do not**:

i) Work on or store personal data or protectively marked data on personal ICT equipment. This includes PCs, laptops, tablets, CDs, DVDs, memory sticks etc
ii) Do not transfer Force information from an encrypted Force device to either an unencrypted or personal device
iii) Send or forward personal data or protectively marked data over the Open Internet or to private email addresses.
iv) Share your password with anyone.
v) Store your password with your ICT equipment.
vi) Hold sensitive conversations, or those involving personal data, in public. Only use secure email or wait until you are back in the office if possible.
vii) Give out personal contact numbers without the owner's consent and must be wary of unidentified callers.

Incident Management

Individuals who become aware that a Police information system or an Information Asset has, or may have been, compromised, must report this, at the first available opportunity, to the Service Desk. Reports should be made in the first instance by e-mail to the Information Security shared mailbox. It is a requirement that they include all relevant details, including, where possible, what information may have been compromised. The types of incident that need to be reported are:

a) Suspected or actual loss of, or unauthorised access to, Protectively Marked material – this includes unauthorised individuals looking at Police system information on a terminal screen or in hard-copy format.
b) Compromise of security measures protecting IT system information – this includes malfunctioning locks, broken shredders, and lost keys to security containers.
c) Suspected virus infection of a system or terminal, including unexpected error messages or warning messages from anti-virus software.
d) Previously unidentified threats to any system information

Related Documents and Appendices

PS 164 Homeworking Policy and PD 625 Homeworking Procedures

Administration

Version Control

Section changed	Details of change

Monitoring and review

Measure	Date/period and process of review

Registered Owner

Owner	Author
Deputy Chief Constable as Senior Information Risk Officer (SIRO)	Information Security Manager