POLICY

Provision of ICT Equipment

Policy owners	ACOs (Resources)
Policy holder	Director of ICT
Author	Director of ICT

Policy No.	15

Approved by

JJNCC	√ 10.09.13.
Legal Services	√ 06.09.13.
Policy owner	√ 24.09.13.
APP	√ 05.09.13.

Note: *By signing the above you are authorising the policy for publication and are accepting accountability for the policy on behalf of the Chief Constables.*

Publication date	03.10.13.
Review date	03.10.15.

Note: *Please send the original Policy with both signatures on it to the Norfolk CPU for the audit trail.*

Index

Legal Basis

(Please list below the relevant legislation which is the legal basis for this policy). You must update this list with changes in legislation that are relevant to this policy and hyperlink directly to the legislation.

Legislation specific to the subject of this policy document

Act (title and year)
Sex Discrimination Act 1975
Race Relations Act 1976
Disability Discrimination Act 1995
Equality Act 2010
Employment Equality (Sexual Orientation) Regulations 2003 and the Equality Act (Sexual Orientation) Regulations 2007
Employment Equality (Age) Regulations 2006
Malicious Communications Act 1988
Communications Act 2003
Criminal Justice and Immigration Act 2008
Protection from Harassment Act 1997
Road Vehicles (Construction and Use) Regulations 1986

Other legislation which you must check this document against (required by law)

Act (title and year)
Human Rights Act 1998 (in particular A.14 – Prohibition of discrimination)
Equality Act 2010
Race Relations Amendment Act 2000
Crime and Disorder Act 1998
H&S legislation
Data Protection Act 1998
Freedom Of Information Act 2000

1. Introduction

1.1 Purpose of Document

The purpose of this document is to state the Norfolk Constabulary and Suffolk Constabulary policy on the provision of ICT equipment and ICT Applications.

1.2 Scope

Throughout this policy 'mobile device' relates to a mobile phone, blackberry, laptop computer or similar device capable of transmitting and receiving data, text or voice over public carriers or Force networks.

This policy applies to all users of ICT equipment, provided by the Joint ICT Department, including but not exclusive to police officers and police staff (permanent and temporary), partners, contractors, consultants, personnel from other forces and agencies.

This policy does not cover the issue and use and security of Airwave Communication devices.

1.3 Assistance

Clarification on any part of this policy or assistance, with obtaining ICT equipment, ICT Applications or other ICT Services, e.g. fault reporting or general help, can be obtained from the ICT Service Desk.

Contact Details: Ext 4747

Email ICTServiceDesk@norfolk.pnn.police.uk

1.4 Accountability

The ICT Department is responsible for the procurement, allocation, delivery, management and maintenance of all ICT equipment in line with this policy. The intention is to ensure that these services:

- Are effective, fit for purpose
- Proactive, and policy-driven
- Reduce bureaucracy
- Provide value for money

2. Provision of ICT Equipment

The Joint ICT Department will only provide ICT equipment based on Force policy and this, in turn, rests upon there being a real business need. All requests for new or additional equipment must be supported by the relevant Head of Department. (Ref; How to Request ICT Equipment and Software).

All Users of ICT Equipment must comply with the joint Information Security Policy and Policy 144 'ELECTRONIC INFORMATION SECURITY (including Network, Patch, Mobile Device and Removable Media Control and Management)'

All Laptops and Mobile devices must have password or pin number access control activated.

2.1 ICT Equipment will be issued to:

- Departments
  Standard Desktop computers and monitors, Fax Machines and Video equipment will normally be issued to a department.

  Shared Laptops will be issued to a nominated manager who will be personally responsible for the equipment.
- Users
  Mobile phones, Mobile Devices, Laptops and Tablet computers will normally be issued to a user. The user will be responsible for the security and safety of the device and will be subject to the cost of replacement of damaged or lost devices in line with policy.
- Centrally Provided Services
  Printing, scanning and photo copying will be provided from centrally managed Multi-Functional Devices (MFD) located at most locations. Where it is not cost effective to provide an MFD local printing facilities will be provided.

2.2 ICT Responsibilities

The ICT Department will coordinate the procurement and issue of all ICT equipment to align with ICT strategy and best value.

The ICT Department will provide a deployment, installation and support service throughout the life of the equipment. Equipment must be used in a manner as described by the Health and Safety in their documents published on their web site.

The ICT Department will configure equipment according to current security guidelines. Please refer to your relevant Force Policy Intranet Site.

The ICT department will repair or replace faulty equipment in adherence to the agreed ICT Service Level Agreement

The ICT department will renew old equipment when required to ensure the equipment performs in line with the business requirement.

All costs for the supply and renewal will be borne by the ICT Department in line with the ICT technical refresh policy.

The ICT Department will record the location of equipment using Service Asset & Configuration Management (SACM).

2.3 Customer Responsibilities

In the event of loss, the device owner must report the loss as soon as practicable to the ICT Service Desk. If the loss of a device is discovered out of ICT Service Desk opening hours it should be reported to the relevant CCR Inspector. Subsequently the loss should be reported to the ICT Service Desk during the next working day. Until the loss (be this through theft or otherwise) is reported the user may be responsible for all calls and use made from that device.

Owners of Force devices must be aware that the loss of the data held on these ICT Equipment can open the Force to serious security issues or reputational damage through the disclosure of information. You must not hold data above RESTRICTED level on mobile devices; do not leave any ICT mobile device unattended in an unsecure area; do not leave your mobile device in your car; take great caution when transferring data from a third-party via memory stick or any other method; report any loss immediately to the ICT Service Desk (if the Service Desk is not open report to the relevant CCR Inspector).

The loss of any ICT equipment that holds data will be reported to the Information Security Manager and to PSD, where appropriate.

All computers and laptops are supplied with an Anti-Virus solution installed. The laptop must be connected and logged in to the force network at least monthly to ensure the Anti-Virus solution is updated.

Any user who suspects or knows their ICT equipment has been compromised by a virus or other malware must cease using the ICT equipment and contact the ICT Service Desk (4747) for advice on further action.

2.4 Reasonable Adjustment Process

If you have a long term health condition or disability that affects the way you do your job, the reasonable Adjustment Process explains how you can obtain items or equipment that will help you, as outlined in the joint Disability Management Policy. (Please refer to your relevant Force Policy Intranet Site).

3. Use of ICT Equipment

Users are reminded that ICT Equipment is issued by the Force for business usage. All usage will be monitored and abuse could lead to disciplinary action up to and including dismissal or criminal investigation where criminal offences are alleged or believed to have been committed (see Usage Monitoring and Auditing).

The following usage is prohibited without exception:

The ICT Equipment must not contain or be used for distributing any harassing, libellous, abusive, threatening, harmful, pornographic, vulgar, obscene, sexist, racist, offensive or otherwise objectionable material of any kind or nature. The ICT Equipment must not be used to distribute Chain Letters (internally or externally).

Users do not knowingly use the ICT equipment to download, publish or access material which is or might be considered to be defamatory, discriminatory, sexist, homophobic, racist, libellous, abusive, intimidating, harmful, pornographic, vulgar, obscene, offensive or otherwise objectionable.

The ICT Equipment must not be used to call chat lines, sports results lines and other equivalent services.

4. Desktop Equipment

The ICT department will provide computers with the standard applications required for the post. This will include Email, Office Applications e.g. word processing, spread sheet and presentations, and access to the intranet in addition to operational policing and organisational applications.

The ICT Department will regularly provide software updates and security patches to all computers connected to the internal network.

All desktop computers will be supplied with a standard flat screen monitor, keyboard and mouse.

Personal use of desktop, laptop and tablet computers is restricted to personal use as defined in the 'Email, Internet and Intranet Use' policy. Personal data must not be stored or processed on these devices.

5. Non Standard Monitors

Throughout this policy 'monitor' relates to either a standard display screen, a non-standard display screen or to one integral in a laptop or tablet.

The ICT Department will coordinate all procurement and supply of monitors.

A standard monitor will be supplied with every new desktop PC as default issue.

Where a laptop has been supplied, as a primary device, this will be with a secondary monitor keyboard and mouse connected via a docking station. Any request for a non-standard secondary monitor will have to meet the requirements detailed in this document.

The ICT Department will only provide larger and secondary monitors based on Force policy and this, in turn, rests upon there being an identified business need.

5.1 Criteria for the Issue of Non-Standard Monitors

Non Standard Monitors will be issued to:

- post holders (e.g. based upon medical need)
  If issued to a post holder, when there is a change of post holder the monitor must be returned to ICT Department by the current post holder for ICT Department to re-issue as appropriate. If the post holder is changing roles, then based upon the original medical criteria, the monitor may be re-issued to the same recipient in his/her new role.

- roles (e.g. Contact and Control Room)
  If issued to a role, the monitor must remain with the desktop/laptop and be used by the new post holder for that role.

5.2 ICT Responsibilities

ICT Department will configure monitors according to current Health and Safety guidelines.

ICT Department will coordinate the collection and reallocation or return of monitors when an individual joins, moves within, or leaves the Force.

All usage will be monitored to ensure that there is a continued business need for a non-standard or supplemental monitor.

Monitors must be used in a manner as described by the Health and Safety in their documents published on their web site.

When a non-standard or supplemental monitor is first issued to a post holder, the post holder will be required to confirm his/her eligibility for the monitor in accordance with this policy and his/her understanding and acceptance of this policy, and will be required to formally acknowledge receipt of the monitor.

5.3 Customer Responsibilities

Post holders are not permitted to pass on monitors directly to any other person. Only monitors issued to roles will be left in place for the incoming post holder.

If a user ceases to be eligible or no longer requires the monitor, he/she must advise the ICT Service Desk so that the monitor can be recovered by ICT.

6. Provision of Mobile Devices

Throughout this policy ‘mobile device’ relates to a mobile phone, blackberry, laptop computer or similar device capable of transmitting and receiving data, text or voice over public carriers or Force networks.

In common with all Force-provided equipment, mobile devices are intended to be used solely for official purposes. It is however recognised that from time to time there may be occasions when it would be appropriate for mobile devices to be used for personal calls/usage. On such occasions the user must repay the cost of calls/usage made. The mobile device must not contain or be used for distributing any harassing, libellous, abusive, threatening, harmful, pornographic, vulgar, obscene, sexist, racist, offensive or otherwise

objectionable material of any kind or nature. It must not be used to distribute Chain Letters (internally or externally).

6.1 Criteria for the Issue of Mobile Devices

Mobile Devices will be issued to:

- Posts (e.g. Force Firearms Officer)
  If issued to a post, when there is a change of post holder, the mobile device must be returned to the ICT Department by the current post holder for the ICT Department to re-issue to the new post holder.
- Roles (e.g. hostage negotiator).
  If issued to a role, the mobile device must be returned to the ICT Department when the current owner of the device ceases to perform the role for which the device was issued. Where appropriate pool devices will be issued for staff to use on a temporary basis.

6.2 Criteria for Mobile Phone Issue

Mobile Phones

Personal issue mobile phones will be available to those who meet one or more of the following criteria:

- Officers and staff who are required to regularly work off-site away from police premises > 2 days per week and it is operationally essential rather than desirable that they need to be contactable by supervisors / colleagues / members of the public (to be agreed by Head of Department).
- Staff who are required to regularly perform ‘on call’ duties, where ‘on call’ teams exist, a single phone will be provided to the team to be shared between the ‘on call’ members.
- It is required for safety, security, operational or efficiency reasons
- Pool phones will be made available to support staff travelling on business

Criteria for Blackberry [PDA] Issue

Personal issue Blackberry will be available to:

- ACPO officers and Heads of Departments.

- A limited number of people in each department who work off-site away from police premises for whom it is operationally essential, rather than desirable, to have immediate access to email on a regular basis and/or outside normal working hours (to be agreed by Head of Department).

- Officers and staff who are on call and need to have immediate access to email. Definition of on call is an accredited on call list held by CCR. Ad-hoc on call arrangements will not qualify.

- Officers and staff having management responsibilities in both forces which require them to travel regularly.

NB: If a Blackberry is issued, a mobile phone will not be issued unless the post/role requires that the individual must have both (e.g. a telephone hands free facility to command incidents from a car, which is not currently permissible with a Blackberry).

Criteria for Laptop Issue

Personal issue laptop computers will be available to:

- ACPO officers and Heads of Departments, if required.

- To a limited number of people in each department for whom it is essential, rather than desirable, to have regular remote access to Force systems and/or to Microsoft Office functions on a standalone basis separate from the Force networked OI system (to be agreed by Head of Department).

- As an alternative to a desktop computer where Heads of Departments can reduce workstation numbers (i.e. desks, chairs and associated furniture and equipment) and space and accommodation requirements by flexible working.

Note: All laptops when provided as a replacement for a standard desktop computer will be supplied with a secondary monitor keyboard and mouse connected via a docking station.

6.3 ICT Responsibilities

The ICT Department will configure devices according to current security guidelines.

ICT will install Desktop and Laptop computers in line with Health and Safety guidance. Desktop and Laptop computers must be used in a manner as

described by the Health and Safety in their documents published on their web site.

The ICT Department will coordinate the collection and reallocation or return of devices when an individual joins, moves within, or leaves the Force.

ICT Department is responsible for management of the telecoms supplier in order to ensure:

- Service levels are appropriate and being met
- Financial charging is accurate and effective
- Value for money is achieved

6.4 Customer Responsibilities

Staff and Officers who use their own vehicles for business use should make use of the earphones provided with the force mobile device, however if these are unsuitable a (force standard) Bluetooth headset will be provided.

If a phone number or mobile device is no longer required by the user e.g. the user is changing post, no longer covering the role or is leaving the Force the device must be returned to the ICT Department. If there is a requirement for the mobile device to be reissued to another user this must be requested using the ICT Request For New Hardware or Software form via the ICT Service Desk and must meet the criteria as defined in section 12 of this policy.

The general intent and expectation in allowing users to make personal calls/usage on Force-provided equipment is that such use should be occasional and infrequent. Personal calling/usage patterns vary considerably from one individual to another, so numerical boundaries cannot be readily defined; however as a guide the number of personal calls/usage made should:

- Result in costs no more than a few pounds per month on average
- Not demonstrate that the primary use of the mobile phone or other device is personal, in which case a tax liability may be incurred.

Users for whom such limitations would be considered onerous are expected to provide a mobile device for their own use, with the Force-provided mobile device used solely for official purposes.

It is illegal to use a hand-held device while driving. It is important to note that any form of distraction is likely to increase the risk of the driver being involved in a road traffic collision. Therefore, it is recommend that Force issued mobile phones are diverted to answer machine/ voice mail whilst driving, unless urgent

operational commitments require phones to be used in a hands-free capacity.

The responsibility for assessing whether it is appropriate to use a hands-free mobile phone remains with the driver at all times.

Personal Usage

- Personal calls should normally be made solely to geographic (01) and mobile (07) numbers only. Exceptionally, calls may be made to non-geographic (08) numbers, but in this case users must be prepared to provide a reasonable explanation for such usage.
- Personal calls to premium-rate and international numbers are not permitted.
- Personal text messages should be very limited in number, and made solely to other mobile phones.
- Premium rate text messages, for example such as used for competition lines and all other premium services, are not permitted.
- Ring-tone downloads are not permitted.

Personal calls/usage must be paid for by the user. Users must reimburse the Force the actual cost of the call/usage, or if it is unreasonably impractical to ascertain the actual cost, then the approximate cost. Arrangements have been made with the mobile service provider for monthly itemised bills to be issued. The procedure for payment is as follows:

- An itemised bill provided to user.
- The user identifies personal calls/usage and calculates the total**,** adding on VAT at the relevant rate.
- All users must notify the Payroll Section of their Finance Department. Deductions will be taken directly from pay. Norfolk Users should use form an AF20 Form and pass this to their force Finance Dept. Suffolk users must email their Force Finance Dept. detailing the personal spend and the VAT.

Users who wish to have a standard amount deducted from each pay period should contact the Payroll Section to arrange. Users should ensure that the periodical deductions at least cover the value of the personal calls/usage (including VAT).

Device bills are routinely dip-sampled and where there is evidence of private use of devices that does not comply with this policy and/or without intent to repay, this will be treated as a disciplinary offence.

Personal Usage – Mobile Devices

Personal use of laptop computers, tablet computers and other mobile devices is restricted to personal use and defined in the ‘Email, Internet and Intranet Use’ Policy and phone calls.

Mobile Devices should not be used to store or process private data.

Restrictions

Force standard car kits for mobile devices will only be fitted to force owned vehicles.

The transfer/port of mobile number or device to a personal contract on termination of employment will not be permitted.

The transfer/port of a number on to a Force account will only be permitted in exceptional circumstances and then only by prior agreement, with the authorisation of the Head of Department and the Director of ICT.

The following usage is prohibited except in emergency:

- Unauthorised access of the internet via a public Wireless Assisted Protocol (WAP) enabled device or the use of 'media mail' and other similar services. Mobile devices will have bars placed on WAP, Premium Rate and international numbers.
- The use of Force issued Subscriber Identity Module (SIM) cards in personal handsets (and vice versa)
- Personal ICT equipment must not be used for Constabulary business and must not at any time be connected to a Force network or computer.

Norfolk Constabulary and Suffolk Constabulary will not reimburse the costs of business calls that are made using a personal mobile phone.

On occasion it may be necessary to use a personal device for business purposes. In such instances users should make the call as brief as possible and ask the contact to call back so as to minimise personal cost.

Use of Airwave handsets to make mobile calls may impinge on service and incur costs. Therefore Airwave handsets should not be used to make mobile phone calls except where this is required for business purpose and where a mobile device is not available. Point to Point Airwave communications can be used between handsets at minimal cost.

Overseas Travel

The standard state of devices will be for international roaming to be disabled. In this state calls cannot be made or received whilst out of the UK.

If travelling abroad as part of Force business, written approval from your Departmental Head must be forwarded to the ICT Service Desk to have international roaming enabled. Devices will not be roaming enabled unless there is a start and an end date provided in the authorisation document

Care must be taken when roaming is enabled to avoid high call costs. When you are using the device abroad you can be charged for any calls that you receive as well as for calls that you make. Roaming call costs are very expensive and best practice tips should be followed to avoid high bills (see below). Note, personal calls and text messages must not be made whilst abroad

General Advice

- Be aware of the cost of calls and if you have a choice then select the most cost effective option available to you.

- Premium rate numbers as well as international numbers are not available on Norfolk Constabulary or Suffolk Constabulary issued devices. To have these facilities enabled written authorisation by Head of Department is required.

- Do not use your mobile phone as a data device e.g. as a modem connected to a laptop.

- Text messaging, like call making and receiving, is more expensive when abroad and usage should be kept to a minimum.

- Text message volumes are monitored with the Professional Standards Department and SMS should not be used as a ‘chat medium’.

- It is an unavoidable fact that the SMS text messaging service is used to propagate ‘spam’, i.e. junk and unsolicited messages. Although receiving these messages does not incur a charge, they often ask you to make a phone call normally to a premium rate number, to claim a prize etc. This type of message should be recognised as spam and deleted immediately. Do not respond or reply to these messages and report any incident to ICT Service Desk who will take appropriate action with the service provider.

- Users of mobile phones can dial an internal numbers within their home force without having to enter the STD code; you only need to dial the 4 digit extension (for example you can dial 4747 for the ICT Service Desk). Users will have to enter the full STD code and number to dial an extension in any other force (for example Norfolk officers contacting a Suffolk Constabulary extension will need to dial the full STD code and number).

- Users should use this facility because it reduces load on the switchboard.

- Users should maintain a list of regular contacts in their mobile phones.
- There are no free calls or texts from mobile phones.

7. Provision of Remote Access

The Remote Access service is to enable staff to perform their official duties from remote locations. This service can only be accessed using a force issued laptop. All users must comply with data security policies.

8. Provision of ICT Application

The Joint ICT Department will only provide ICT applications based on Force policy and this, in turn, rests upon there being a real business need. All requests for new or additional applications must be supported by the relevant Head of Department.

Local Applications, for example Visio, Adobe Suite, Graphics Suites and other off the shelf applications can be requested using the same process for requesting ICT Equipment. (Ref: How to Request ICT Equipment and Software).

Corporate Systems and large scale applications should be requested via the Strategic Change department.

9. Financial Policy and Management

ICT equipment, accessories and software will be procured by the ICT Department on behalf of users. The ICT Department will also replace devices as upgrades become necessary.

All variable associated costs (e.g. purchase, fitting, repair, call charges etc.) will be borne by the ICT Department.

If the loss and/or damage is due to lack of care by any individual, he or she may be required to pay for the damage or replacement if necessary.

10. Auditing

When a device is first issued to a user, the user will be required to formally sign for the device, see Appendix C.

Users are not permitted to pass on devices directly to any other person. If a user ceases to be eligible or no longer requires the device, or needs to pass the device on to a successor post-holder, he/she must return the device to the ICT Department, who will formally acknowledge receipt back.

Users must also provide confirmation to the ICT Service Desk annually, which will be prompted by the ICT Department, to confirm that they are still in possession of the device, that they are still eligible to use it in accordance with this policy, and that they still require it. If such confirmation is not received within one month of the annual renewal date then ICT Department will remotely disable the device so that it can no longer be used. The user who last formally acknowledged receipt of the device will be asked to account for it and if satisfactory account cannot be given will be charged the cost of a replacement.

All usage will be monitored and abuse could lead to disciplinary action up to and including dismissal or criminal investigation where criminal offences are alleged/believed to have been committed.

Mobile usage will be monitored and the ICT Department will issue periodic exception reports to highlight high and low utilisation and will challenge the need for a device where appropriate. The owning department is responsible for reviewing the on-going need for an individual to have a device.

ICT Department will issue a monthly report of mobile usage to device users to check for personal usage. Details of how to reimburse personal usage can be found in section 7.3.1 of this document. You should remember to add VAT at the prevailing rate.

ICT and Professional Standards Departments will monitor individual device usage for exceptions.

The ICT Department will audit all devices to ensure:

- All devices are accounted for
- Current owner/location is known;
- Owners of devices with privileged access (MTPAS / ACCOLC) are known
- Devices allocated to individuals are known

11. How to Request ICT Equipment and Software

Requests for ICT equipment, mobile devices and remote access for Norfolk Constabulary staff and officers should be submitted via the ICT Request for New Hardware or Software Form available on the ICT intranet page.

Suffolk Constabulary staff and officers should complete the ICT Request for New Hardware and Software form available on the Suffolk ICT Intranet Home page.

The requester must complete the form fully and ensure that the criteria, for the issue of the requested equipment, is evidenced.

The requester must submit the completed form to their Head of Department (Superintendent or above) for authorisation. If it is authorised the completed form must be emailed to the ICT Service Desk where the request will be logged on the ICT Service Management system.

The request will be reviewed by the relevant ICT Senior Manager and the decision will be fed back to the requester.

If the request is rejected the Requester can appeal to Director of ICT. The final decision will rest with the Director of ICT

If it is approved by ICT and the Finance is authorised ICT will contact the Requester to discuss requirements. If the equipment is not a stock item orders will be raised.

Upon availability of the equipment ICT will contact the requester to arrange installation and the location of the equipment will be recorded in the Configuration Management Database.

The ICT Service Management system will be updated at all stages to ensure that the request is managed efficiently.

Appendix A. ICT Request New Hardware & Software Process