POLICY

Provision of ICT Equipment

Policy Owner	DCCs Norfolk & Suffolk Constabularies
Policy Holder	Director of ICT
Author	Director of ICT

Approved by

Legal Services	Not required
Policy Owner	4 December 2018
JJNCC	4 December 2018

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	5 December 2018
Review date	5 December 2022
APP checked	Yes
College of Policing Code of Ethics checked	Yes

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
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
Health and Safety (Display Screen Equipment) Regulations 1992 as amended by the Health and Safety (Miscellaneous Amendments Regulations) 2002

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
Crime and Disorder Act 1998
Health and Safety at Work etc. Act 1974 and associated Regulations
General Data Protection Regulation (GDPR) and Data Protection Act 2018
Freedom Of Information Act 2000
The Civil Contingencies Act 2004

Other Related Documents

- Business Continuity policy

1. Introduction

Purpose of Document

1.1 The purpose of this document is to state the Norfolk and Suffolk Constabularies' policy on the provision of information, communications and technology (ICT) equipment and ICT Applications.

Scope

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

1.3 'Smart phone' relates to devices that perform the functions of a mobile phone and also enable controlled connection to force applications, e.g. email.

1.4 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.

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

Assistance

1.6 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

Accountability

1.7 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 and fit for purpose;
- Are proactive and policy-driven;
- Reduce bureaucracy;
- Provide value for money.

2. Provision of ICT Equipment

2.1 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.

2.2 All Users of ICT Equipment must comply with the joint Information Security Policy, Health and Safety Display Screen Equipment Arrangement' and 'Electronic Information Security (including Network, Patch, Mobile Device and Removable Media Control and Management)'.

2.3 All Laptops and Mobile devices must have password or PIN number access control activated, without exception, to comply with national information security codes of connection.

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, smart 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.

ICT Responsibilities

2.4 The ICT Department will coordinate the procurement and issue of all ICT equipment to align with local, regional and national ICT strategy and best value.

2.5 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 Health and Safety (Display Screen Equipment) Regulations 1992 and Health and Safety Display Screen Equipment Arrangement as published on their intranet site.

2.6 The ICT Department will configure equipment according to current security guidelines.

2.7 The ICT department will repair or replace faulty equipment in response to requests made to the ICT Service Desk. Requests will be graded based

on their operational impact and organisational priorities at the time of submission.

2.8 The ICT department will renew old equipment, when required, to ensure the equipment performs in line with the business requirement and equipment replacement guidelines / timescales. All costs for supply and renewal will be borne by the ICT Department.

2.9 The ICT Department will record the location of equipment using Service Asset & Configuration Management (SACM – provided by Marval MSM). ICT will carry out audits of offices and users to ensure equipment is present and being used in line with force policy.

Customer Responsibilities

2.10 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. The loss should then 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 the usage of the device.

2.11 Personal issue devices must be returned to ICT when a user changes role or leaves the organisation.

2.12 Owners of force devices must be aware that the loss of data held on ICT Equipment can open the force to serious security issues and/or reputational damage through the disclosure of information.

The following must therefore be observed at all times:

- Data which is already marked as RESTRICTED under the old GPMS marking scheme must not be held on mobile devices.
- Data marked as OFFICIAL-SENSITIVE and above under the current GPMS marking scheme must not be held on mobile devices.
- Mobile devices must not be left unattended in an unsecure area, including any vehicle.
- Great caution must be taken when transferring data from a third party via USB memory devices, SD cards etc. (or any other method) and any loss must be reported immediately to the ICT Service Desk. If the Service Desk is not open the report should be made to the relevant CCR Inspector.

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

2.14 Due to the serious nature of cyber security threats, it is imperative that all devices are regularly connected to the Constabulary's network. This will ensure that all anti-virus solutions and patches can be updated. Connection should be made at least monthly, as a minimum. Any devices not connected within 90 days will be immediately removed from the network to protect the device and the Constabulary network from any vulnerability.

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

Reasonable Adjustment Process

2.16 If an individual has a long term health condition or disability that affects the way they perform their role, this should be accommodated through a process initiated by the Workplace Health, Safety and Wellbeing Teams.

3. Use of ICT Equipment

3.1 All ICT equipment including (but not limited to) desktops, laptops and tablets are provisioned for business use. However, if the occasion arises where it becomes necessary for personal use, the user must adhere to the 'Email, Internet and Intranet Use' policy. Personal data must not be stored or processed on these devices. All usage will be monitored and abuse or breach of the policy requirements 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:

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

3.3 Users must 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 unless for a specific policing purpose.

3.4 The ICT Equipment must not be used to call or access chat lines, sports results lines or any other equivalent service.

3.5 The ICT equipment must not be used for any activity in connection with a business interest.

4. Desktop Equipment

4.1 The ICT department will provide computers with the standard applications required for a user to fulfil their post. This will include email, office applications such as word processing, spreadsheets and presentations and access to the intranet, in addition to operational policing and organisational applications.

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

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

5. Monitors

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

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

5.3 Standard monitors will be supplied with every new desktop PC as default issue.

5.4 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 policy.

5.5 Larger display screens will require a business case to support the purchase of such equipment. This business case must demonstrate why the standard issue screens are insufficient for the needs of the requestor.

Criteria for the Issue of Non-Standard Monitors

5.6 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.

ICT Responsibilities

5.7 The ICT Department will configure monitors according to current Health and Safety (Display Screen Equipment) Regulations 1992 and Health and Safety Display Screen Equipment Arrangement as published on their intranet site.

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

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

Customer Responsibilities

5.10 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.

5.11 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.

5.12 Monitors must be used in a manner as described by Health and Safety (Display Screen Equipment) Regulations 1992 and Health and Safety Display Screen Equipment Arrangement as published on their intranet site.

5.13 Laptops and mobile devices should not be used for prolonged periods without ensuring they are set up correctly and in accordance with the Health and Safety (Display Screen Equipment) Regulation 1992 and Health and Safety Display Screen Equipment Arrangement as published on their intranet site.

6. Provision of Mobile Devices

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

6.2 In common with all equipment provided by the force, 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. In these circumstances, Users should refer to the Email, Intranet & Internet Use policy. The mobile device must not contain or be used for accessing or distributing any harassing, libellous, abusive, threatening, harmful, pornographic, vulgar, obscene, sexist, racist, offensive or otherwise objectionable material of any kind or nature unless for a specific policing purpose. It must not be used to distribute Chain Letters (internally or externally).

Criteria for the Issue of Mobile Devices

6.3 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.

Criteria for Mobile Phone Issue

6.4 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 more than 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 Smart Phone Issue

6.5 Personal issue smart phones will be available to:

- ACPO officers and Heads of Departments.

- A limited number of people in each department who work off-site and 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.

Criteria for Laptop \ Tablet Issue

6.6 Personal issue laptop computers will be available to roles that have been identified as requiring the ability to work remotely or across multiple locations, and 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.

6.7 Where a laptop is issued, this will become the user's primary device and, as such, a desktop is required to be returned to ICT for re-use or recycling.

6.8 All laptops \ tablets, 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, where appropriate.

ICT Responsibilities

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

6.10 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 Health and Safety (Display Screen Equipment) Regulations 1992 and Health and Safety Display Screen Equipment Arrangement as published on their intranet site.

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

6.12 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.

Customer Responsibilities

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

6.14 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 Self Service Portal (which can be accessed from the Windows Start Menu or the ICT Intranet page) and must meet the criteria defined in this policy.

6.15 Force issued mobile phones should not be used for personal reasons except under exceptional circumstances. Personal use of the force mobile phone may result in a tax liability.

6.16 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.

6.17 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 devices are diverted to answer machine / voicemail whilst driving, unless urgent operational commitments require phones to be used in a hands-free capacity.

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

Personal Usage – Mobile Devices

6.19 Personal use of laptop computers, tablet computers and other mobile devices is restricted, including personal phone calls. However, if the occasion arises where it becomes necessary for personal use, the user must adhere to the 'Email, Internet and Intranet Use' policy.

6.20 Mobile Devices should not be used to store or process private data, including music and photos.

Restrictions

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

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

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

The following usage is prohibited (except in an emergency):

- Unauthorised internet usage / access or the use of 'media mail' and other similar services. Mobile devices will have bars placed on Premium Rate and international numbers.
- The use of force issued Subscriber Identity Module (SIM) cards in personal handsets (and vice versa).
- Personal ICT equipment (including smartphones, USB sticks, computers and tablets) must never be used for Constabulary business and must not at any time be connected to a force network or computer. In exceptional circumstances 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. Norfolk and Suffolk Constabularies will not reimburse the costs of business calls that are made using a personal mobile phone.
- Airwave handsets should not be used to make mobile phone calls except in exceptional circumstances for business use or where a mobile device is not available. Doing so may cause negative impacts on service and additional costs to the Constabularies. Point to Point Airwave communications can be used between handsets at minimal cost.

Overseas Travel

6.24 International roaming will be disabled as standard procedure on all devices. This means calls cannot be made or received whilst outside of the UK.

6.25 If travelling abroad as part of force business, written approval from the relevant 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.

6.26 Care must be taken when roaming is enabled to avoid high call costs. When using the device abroad, charges may be incurred from calls received as well as made. Roaming call costs are very expensive and best practice should be followed to avoid high bills – see general advice below. Note that personal calls and text messages must not be made whilst abroad.

General Advice

- Be aware of the cost of calls and if, if a choice is available, select the most cost effective option.
- Premium rate numbers as well as international numbers are not available on Norfolk or Suffolk Constabulary issued devices. To

have these facilities enabled, written authorisation by Head of Department is required.

- Mobile phones must not be used 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 within 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 invite the recipient 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 the ICT Service Desk who will take appropriate action with the service provider.

- Users with a force smart phone should maintain an up to date list of regular contacts in the phone. In the event of a problem with the phone (such as breakage), this provides a backup for contacts – these handsets are backed up to Exchange which allows all contacts from the phone to be accessible through Microsoft Outlook.

- Users who do not have a force issued smart phone should find an alternative way of backing up contacts to prevent loss in the event of a problem with the phone (such as breakage).

7. Provision of Remote Access

7.1 The Remote Access service is to enable staff to perform their official duties from remote locations. This service is automatically accessible to a force issued laptop as they are all Direct Access enabled. Any laptop which is not force issued will be enabled to the network through use of a CAG / Any Connect token which can be requested through the ICT Self Service Portal (accessed from the Windows Start Menu or the ICT intranet page). All users must comply with the Remote Access Policy and data security policies.

8. Provision of ICT Applications

8.1 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 and agreed by the Director of ICT.

8.2 Local Applications, e.g. Visio, Adobe Suite, Graphics Suites and other 'off the shelf' applications can be requested using the same process for requesting ICT Equipment.

9. Financial Policy and Management

9.1 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 in line with equipment replacement guidelines and timescales.

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

9.3 If the loss and / or damage results from lack of care by any individual they may be required to pay for the damage or replacement, if necessary. Any accidental damage caused through use of equipment in an operational setting / circumstances will not result in a penalty.

10. Auditing

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

10.2 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 and then re-issue the device, as required.

10.3 ICT will perform regular audits to ensure devices are being used. Users will be asked by the ICT Department to provide confirmation to the ICT Service Desk 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.

10.4 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.

10.5 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.

10.6 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;
- The current owner / location is known;
- Owners of devices with privileged access (MTPAS / ACCOLC) are known;
- Devices allocated to individuals are known;
- Devices have appropriate security updates.

11. How to Request ICT Equipment and Software

11.1 Requests for ICT equipment, mobile devices and remote access for all staff and officers should be submitted via the ICT Self Service Portal which can be accessed from the Windows Start Menu or the ICT intranet page.

11.2 The requester must complete the form fully and ensure that all criteria for the issue of the requested equipment are evidenced.

11.3 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.

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

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

11.6 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.

11.7 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.

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