JOINT NEGOTIATING COUNCIL
EDUCATION AUTHORITY

28 September 2018

To JNC Council Members
MSO/TUSO

JOINT NEGOTIATING COUNCIL CIRCULAR NO. 250

ACCEPTABLE USE OF ICT POLICY

The Joint Secretaries have considered and agreed the attached Acceptable Use of ICT Policy.

The policy incorporates amendments to reflect changes in the use of technology in the workplace with additional references including internet use, social networking sites, mobile computing, removable media and software use.

This policy updates and replaces JNC Circular No 97 Internet and Email Usage (dated 29 July 2003) which should be DELETED.

A copy of the Policy is attached as Appendix A to this circular.

Management Side Secretary
R McGreevy

Trade Union Side Secretary
K Bannon

Trade Union Side Secretary
A Speed

Trade Union Side Secretary
D Walker

Trade Union Side Secretary
M Keenan

Council Secretary: Grainne McClean
County Hall, 182 Galgorm Road, Ballymena BT42 1HN Telephone: 028 9041 3166

Acceptable use of ICT policy

Author: Technical Standards Group

September 2018

Contents

		Page
1.	Purpose of Policy	2
2.	Scope of Policy	2
3.	Structure of Policy	2
4.	The Acceptable Use of ICT Policy	3
5.	Common Policy	5
6.	Email Use	7
7.	Internet Use	8
8.	Mobile Computing	10
9.	Removable Media	11
10.	Software Use	13
11.	Review	15
12.	Appendix 1	15

1. PURPOSE OF POLICY

This document sets out the policy of the Education Authority (EA) in relation to the use of all Information and Communications Technology (ICT) resources owned or operated by the organisation.

Our IT and communications systems are intended to promote effective communication and working practices within our organisation. This policy outlines the standards you must observe when using these systems, the circumstances in which we will monitor your use, and the action we will take in respect of breaches of these standards.

Misuse of IT and communications systems can damage the business and our reputation. Breach of this policy may be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

The policy is intended to protect the interests of the organisation as well as the interests of staff and authorised third-parties.

2. SCOPE OF POLICY

The policy applies to all staff of EA, contractors and their employees and others given access to use the organisation's ICT resources. In the context of this policy, the use of the term "staff" includes all users of EA ICT resources.

The policy applies to all ICT resources owned, leased or supported by EA. This includes equipment supplied under private finance arrangements. The policy also applies to non-organisational equipment or facilities used to obtain access to EA ICT resources at home or other remote locations, including personal ICT equipment. This policy applies at any time, including outside office hours, and regardless of whether EA's equipment or ICT resources are used insofar as a breach of policy may occur. The organisation may permit staff to use resources for personal use in their own time providing that such use does not compromise the security of official data, result in increased costs or delays or have any negative impact or liability on the organisation or its network or on the effective discharge of official business.

Personal use is defined as any use of ICT resources that does not stem from a requirement directly relating to the officer's official duties. Own time is when an individual is not on duty, such as before signing in, after signing out or during lunch or other officially sanctioned breaks. This use is granted at the discretion of management and may be withdrawn at any time for operational reasons or if misuse is suspected or detected.

3. STRUCTURE OF THE POLICY

The Acceptable Use of ICT Policy contains a number of distinct sections. Section 5 (Common Policy) includes aspects of policy that are applicable to all other sections. It is the responsibility of staff to ensure that they have read all sections. These are as follows:

Section 5	Common Policy
Section 6	Email Use
Section 7	Internet Use
Section 8	Mobile Computing
Section 9	Removable Media
Section 10	Software Use

4. ACCEPTABLE USE OF ICT POLICY

All staff who use or intend to use the organisation's ICT resources for any purpose will be required to acknowledge that they have read, understood and will adhere to the organisation's Acceptable Use of ICT Policy and any related policies which are published on the EA staff intranet. Such undertakings should be renewed if these policies change. Failure to comply with the requirements of the organisation's policy and other relevant policies may result in disciplinary action, including dismissal. Training and testing of understanding of the Acceptable Use of ICT Policy will be provided via online eLearning.

4.1 Personnel responsible for implementing the Policy

Responsibility for monitoring and reviewing the operation of this policy and making recommendations for change to minimise risks lies with the EA's Director of Finance and ICT.

All managers and section heads have a specific responsibility for operating within the boundaries of this policy, ensuring that all staff understand the standards of behaviour expected of them and taking action when behaviour falls below its requirements.

Any misuse of EA's ICT resources should be reported to the Director of Finance and ICT. Any questions regarding the content or application of this policy should be directed to the Director of Finance and ICT.

4.2 Regulatory Framework

Use of EA's ICT resources is subject to a number of pieces of national legislation. A summary of this legislation is set out below. This list is subject to any legislation coming into force following the date of issue of the Policy.

General Data Protection Regulations
Freedom of Information Act 2000
Regulation of Investigatory Powers Act 2000
The Lawful Business Practice Regulations 2000
The Computer Misuse Act 1990
Copyright, Designs and Patents Act 1988
Health and Safety at Work (NI) Order 1978
Health and Safety (Display Screen Equipment) Regulations (NI) 1992
The Obscene Publications Act 1959 &1964
The Protection of Children Act 1978
Human Rights Act 1998
Breach of Communications Act 2003
Disability Discrimination Act 1995
Employment Equality (Age) Regulations (NI) 2006
Fair Employment and Treatment (NI) Order 1988
Part Time Workers (Prevention of Less Favourable Treatment) Regulations (NI) 2000
Sex Discrimination (NI) Order 1976
Malicious Communications (NI) Order 1988
Protection from Harassment (NI) Order 1997
Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
Electronic Communications Act 2005
Communications Act 2003
Criminal Justice and Immigration Act 2008
Sexual Offences Act 2003

Compliance with the terms of this policy will enable EA staff to comply with this legislation, as it relates to the use of ICT.

4.3 Monitoring and Privacy

Staff should note that, as is permitted by legislation, EA will monitor and review Internet, email and other electronic communications and will analyse usage patterns and may publish resultant data (traffic monitoring). The organisation will also monitor the content of emails, attachments and files as and when this is considered necessary in order to ensure the integrity of the organisation's systems and that users are complying with all relevant usage policies and guidance (content monitoring). Use will be routinely monitored and may be specifically monitored at any time when this is deemed necessary for compliance or other reasons, including the prevention or detection of alleged wrongdoing or to comply with any legal obligation. Monitoring of an individual's use of ICT will only be conducted where there are substantial grounds to do so.

The organisation reserves the right to inspect and examine any ICT equipment (including personally owned equipment) used on official premises for the conduct of official business or connected in any way to the organisation's network in order to ensure compliance with the organisation's usage policies.

External devices attached to the EA network will be routinely monitored to protect the security of the EA network, and the resulting audit reports may be used for investigation of possible breaches or misuse of ICT resources.

It may be necessary, for business or other reasons, to obtain access to the ICT equipment, mailbox or network share of a member of staff who is absent from work. Access in these circumstances will be facilitated by ICT staff upon receipt of appropriate managerial authorisation, and the member of staff will be duly notified of access on their return to work.

Users of EA's ICT facilities should therefore be aware and must accept as a condition of use that their usage of these facilities may be monitored. Monitoring is carried out to the extent permitted or as required by law and as is necessary and justifiable for business purposes. Monitoring of an individual's use of ICT must only be carried out where Assistant Director Level authorisation, on a case by case basis, has been provided. ICT staff must not access details of an individual's ICT use without Assistant Director Level authorisation.

4.4 Standards of Acceptable Use

Misuse of the EA ICT facilities may be dealt with under our Disciplinary Procedure, and in some circumstances can be a criminal offence and any such action will be treated very seriously which is likely to result in summary dismissal. Excessive personal use of the EA ICT facilities within working hours may also be dealt with under EA Disciplinary Procedures.

Where evidence of misuse is found EA may undertake a more detailed investigation in accordance with our Disciplinary Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation. If necessary such information may be handed to the police in connection with a criminal investigation.

Inappropriate material or remarks may include but are not limited to any content of a pornographic, violent or offensive nature or those which breach any discrimination laws or

offend any 'protected characteristics' to include but not limited to, sex, race, disability, sexual orientation, religion or belief, age or gender reassignment; in pictures, cartoons, words, sounds or moving images whether or not purporting to be of a humorous nature. In cases of harassment, a claim by a user that he/she had not intended to harass or cause offence will not in itself constitute an acceptable defence.

Users should be aware that the possession of child pornography is a criminal offence. EA will fully co-operate with law enforcement authorities to identify and take action against any member of staff accessing, possessing or disseminating such material. Individuals found to have been involved in any way in the access, possession or dissemination of child pornography using EA's ICT systems may be dealt with under our Disciplinary Procedure and, in serious cases, most likely to face a charge of gross misconduct leading to summary dismissal, irrespective of whether or not they are prosecuted or convicted under the criminal law.

4.5 Disciplinary Action

Users of EA's ICT facilities must respect the privacy and legitimate rights of others, as would be appropriate in any other form of work activity. Individuals will be held accountable for any misuse, and may be subject to disciplinary action up to and including termination of employment. Access to ICT facilities may be withdrawn at any time as a result of, or pending the outcome of, investigations into suspected misuse.

EA must act within the law, which means it has in turn to ensure that members of staff are doing so, by enforcing the regulatory framework as explained in this policy. Therefore any breach of this regulatory framework may be treated by the organisation as a serious disciplinary matter. Where circumstances dictate, the organisation will inform and co-operate with relevant legal enforcement bodies. Users should note that they might be personally liable to prosecution and subject to personal claims for damages should their actions be found to be in breach of the law. No indemnity will be afforded to any member of staff who breaches this policy or the law.

4.6 Copyright

Users of EA's ICT facilities must respect copyright, software licensing regulations and property rights. Staff are reminded that copyright in all material produced in the course of official duties belongs to EA. Staff shall therefore take appropriate steps to ensure that EA's copyright ownership is protected when emailing or publishing material in any form.

4.7 Consultation with Trade Unions

The terms of this policy have been agreed between the Trade Union Side of the Joint Negotiating Council and EA.

This policy does not form part of any employee's contract of employment and it may be amended at any time.

5. COMMON POLICY

The EA Default Domain Policy will automatically enforce password age, complexity and account lockout settings for all network accounts. However, users are required to comply with the general terms of the Acceptable Use of ICT Policy as set out below in order to ensure that the security of EA computer systems and the information they contain is not compromised in any way.

You are responsible for the security of the equipment allocated to or used by you, and must not allow it to be used by anyone other than in accordance with this policy.

You are responsible for the security of any computer terminal used by you. You should lock your terminal or log off when leaving it unattended or on leaving the office, to prevent unauthorised users accessing the system in your absence.

Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without first consulting the EA ICT Service.

You should use passwords on all IT equipment, particularly items that you take out of the office. You must keep your passwords confidential and change them regularly. You must not use another person's username and password or make available or allow anyone else to log on using your username and password unless authorised by the EA ICT Service. On the termination of employment (for any reason) you must provide details of your passwords to the EA ICT Service and return any equipment, key fobs or cards.

If you have been issued with a laptop, tablet or smart phone, you must ensure that it is kept secure at all times, especially when travelling. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event of loss or theft. You should also be aware that when using equipment away from the workplace, documents may be read by third parties, for example, passengers on public transport.

5.1 What users MUST do

At all times users must:

- keep all passwords and user IDs confidential and secure (the sharing of user IDs or passwords is prohibited); and
- inform the EA ICT Service Desk immediately if they believe their account details have been compromised.

5.2 What users must NOT do

At no time may users:

- leave an unattended machine logged on, which could lead to unauthorised use of accounts and user IDs (computers must be manually locked before being left unattended);
- use EA ICT facilities to commit infractions such as harassment/bullying, discrimination, defamation, unauthorised public representation, misappropriation or infringement of intellectual property rights or misuse of EA assets or resources;
- intentionally access, store, distribute, edit, record, or reproduce (on screen, hardcopy or via audio) any kind of inappropriate material on EA ICT facilities;
- compromise the security or confidentiality of organisational data, customer data or any other data covered by organisational policies and procedures;
- engage in any political advocacy or the unauthorised endorsement or appearance of endorsement of any commercial product or service;

- use EA ICT facilities to carry out any activities for personal gain, including share dealing or monitoring, investment portfolio management, or gambling;
- knowingly or negligently propagate any virus or malicious program designed to infiltrate a system without the user's knowledge to gather information or corrupt data;
- use EA ICT facilities to disable or overload any computer system or network;
- disable, defeat or circumvent firewalls or any EA ICT security facility intended to protect the privacy or security of systems, networks or users;
- use EA facilities to copy, download or forward non-business related software or data, including music, graphics, videos, text, games, entertainment or pirated software;
- cause reputational damage from inappropriate email or other ICT uses;
- gain access to restricted areas of the network, or to any password protected information, except as authorised in the proper performance of duties; or
- use EA ICT facilities to violate in any way laws and regulations applicable in Northern Ireland.

6. EMAIL USE

For the purposes of this policy, electronic mail or email is defined as all technologies used to transmit messages or data electronically. EA mail server settings will automatically enforce organisational policy in relation to email encryption, retention and storage. However, users must at all times have due regard to policy as stated below.

We monitor all e-mails passing through our system for viruses. You should exercise particular caution when opening unsolicited e-mails from unknown sources or an e-mail which appears suspicious (for example, if it contains a file whose name ends in .exe). Inform the EA ICT Service immediately if you suspect your computer may have a virus. We reserve the right to delete or block access to e-mails or attachment in the interests of security. We also reserve the right not to transmit any e-mail message.

You must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, or otherwise inappropriate e-mails. Anyone who feels that they have been harassed or bullied, or are offended by material received from a colleague via e-mail should inform their line manager OR the Human Resources Directorate.

You should take care with the content of e-mail messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Staff should assume that e-mail messages may be read by others and not include anything which would offend or embarrass any reader, or themselves, if it found its way into the public domain.

E-mail messages may be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an e-mail cannot be recovered for the purposes of disclosure. All e-mail messages should be treated as potentially retrievable, either from the main server or using specialist software.

6.1 What users MUST do

At all times users must:

- identify themselves honestly, accurately and completely;
- maintain the clarity, consistency and integrity of the organisation's image, and avoid making any inferences that may prove inappropriate from the organisation's perspective; and
- report immediately to their line manager or, if appropriate, to Human Resources the receipt of inappropriate or offensive material delivered via email.

You should return any wrongly-delivered e-mail received to the sender.

6.2 What users must NOT do

At no time may users:

- send or forward files containing sensitive or personal organisation data unless the data is first encrypted using a security product approved by the organisation;
- arrange to auto-forward e-mails from an organisation account to a personal email account or from a personal email account to an organisation account (emails received into an organisation account may be forwarded once their contents have been checked to ensure that the forwarding of the emails does not contravene policy in respect of protectively marked material);
- access the mailbox of an absent member of staff or issue emails in the name of another member of staff without appropriate managerial approval;
- use non-organisational email accounts for the transaction of EA business;
- send or forward private e-mails at work which you would not want a third party to read;
- send or forward chain mail, junk mail, cartoons, jokes or gossip;
- contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding e-mails to those who do not have a real need to receive them;
- download or e-mail text, music and other content on the internet subject to copyright protection, unless it is clear that the owner of such works allows this; or
- send confidential messages via e-mail or the internet, or by other means of external communication which are known not to be secure.

7. INTERNET USE

Staff should be aware that all Internet access using the EA network is subject to content filtering and access to sites containing high-risk and inappropriate material will be routinely blocked. Users attempting to access an Internet website categorised in this way will receive a system notification. Access to blocked sites will only be permitted on written authorisation from a Line Manager.

All Internet access will be routinely monitored and patterns of usage analysed for reporting purposes. Staff should be aware that individual usage may be specifically monitored at any time when this is deemed necessary for compliance or other reasons, including the prevention or detection of illegal activities.

In order to preserve network and data security, EA may prevent connection to the Internet of certain machines holding sensitive data or applications or restrict use of Internet features such as file transfers.

Social Networking Sites

EA recognises that the internet provides unique opportunities to participate in interactive discussions and share information on particular topics using a wide variety of social media, such as Facebook, Twitter, blogs and wikis. However, employees' use of social media can pose risks to EA's confidential and proprietary information, and reputation, and can jeopardise EA's compliance with legal obligations.

To minimise these risks, to avoid loss of productivity and to ensure that our IT resources and communications systems are used only for appropriate business purposes, EA requires employees to adhere to EA's Social Media Policy.

7.1 What users MUST do

At all times users must:

- report immediately any indication of virus or other attack to the EA ICT Service Desk;
- respect copyright, software licensing rules and property rights, and download only software with direct business use; and
- schedule communication-intensive operations, such as large file transfers, video downloads and mass emailing for off-peak times wherever possible.

7.2 What users must NOT do

At no time may users:

- knowingly connect to any Internet site that contains inappropriate material. If such a site is inadvertently accessed, users will immediately disconnect from the site regardless of whether that site had been previously deemed acceptable by any screening or rating program. Such inadvertent connections must be reported immediately to the EA ICT Service Desk so that appropriate action to bar access to the site can be taken and to safeguard the individual in the event of any subsequent investigation;
- transfer via the Internet, or store on the Internet, any files containing sensitive or personal organisation data unless the data is encrypted and adequately protected by security mechanisms approved by EA ICT;
- make excessive use of Internet facilities to the detriment of official duties; or
- use Internet proxy sites to bypass EA monitoring systems.

7.3 Personal Internet Use

EA may permit staff to use Internet facilities for personal use, in their own time, providing that such use does not compromise the security of official data, result in increased costs or delays or have any negative impact on the EA network or on the effective discharge of official business.

The facility is granted at the discretion of management and may be withdrawn at any time for operational reasons or if misuse is suspected or detected. All Internet use is subject to monitoring and such monitoring does not differentiate between official and personal use.

Subject to EA policies in relation to personal use, staff may in their own time use the Internet for the occasional purchase of goods and services provided payment is made by the

individual and delivery of items purchased is to a private address. Staff must not use work-related email accounts or addresses for personal transactions.

Staff must not create any unauthorised contractual liability on the part of EA. EA does not accept any responsibility for the security of credit card details or any other payment method used. EA does not accept any liability for financial loss, whether as a result of fraud or otherwise, suffered while using EA systems for personal transactions. All such use is entirely at the individual's own risk.

Staff may make occasional use of EA facilities for on-line banking. All such use will be at the individual's own risk. EA cannot accept any liability for losses or for any other liabilities arising out of such transactions, howsoever caused.

8. MOBILE COMPUTING

The purpose of this policy is to ensure that effective measures are in place to protect against the risks of using mobile computing and communication facilities. Specifically, the objectives of the policy are to:

- provide secure remote access to EA information systems;
- preserve the integrity and confidentiality of EA information systems; and
- manage the risk of serious financial loss, loss of confidence and other serious business impact which may result from failure in security.

Mobile computing is a generic term describing the facility to use ICT devices while not in a networked location. The policy applies to authorised users connecting remotely to the EA network to access internal network resources. For example, to read or send email, to view intranet web resources or to transfer information between mobile devices while not in an EA location.

The following list indicates the types of equipment covered by this policy:

- Laptops and notebooks
- Mobile phones
- Smart phones
- Tablet Computers

A definition of each of these devices is included in Appendix 1.

Users are reminded that wireless networks and public networks are less secure than EA's wired network environment.

Mobile devices are vulnerable to theft, loss or unauthorised access when taken outside of EA buildings. Appropriate forms of access protection, including disk encryption, will therefore be enforced by EA to prevent unauthorised access to their contents.

EA will not be responsible for providing technical support for equipment, network or internet connections belonging to users or to another organisation.

Specific devices or families of devices may be prohibited from use for accessing corporate data.

8.1 What users MUST do

At all times users must:

- store equipment out of view in a locked place, users are responsible for mobile equipment, systems and information in their possession;
- immediately report loss of any mobile device containing sensitive data, or any other security breach, to the EA ICT Service Desk;
- ensure that screens are appropriately protected from the view of unauthorised persons;
- ensure that all information received or transmitted in public places is done so securely; and
- ensure that all information held on any mobile device is securely erased before the device is reassigned to another user or to another purpose.

8.2 What users must NOT do

At no time may users:

- remove EA information assets off-site on laptops or other mobile devices without proper authorisation;
- leave mobile equipment unattended in insecure areas;
- transfer any file containing sensitive or personal data to a mobile device (data stored on laptops and other mobile storage devices should be kept to a minimum to reduce risk and impact should a breach of security occur);
- transfer any file containing sensitive or personal data to a mobile device unless the data is first encrypted using a security product approved by the organisation;
- transfer any file containing sensitive or personal data to or from a mobile device using Bluetooth or other wireless communication technologies;
- process sensitive or personal data in public places, such as on public transport, when using a laptop or other mobile device;
- transfer business-related data to Internet-based storage space provided by a third-party unless specifically authorised to do so;
- leave their equipment unattended or leave a computer connected to the EA network unattended at any time;
- leave ICT equipment and media unattended in public places, portable computers should be carried as hand luggage when travelling;
- use personal laptops and home computers for business activities without appropriate security measures, including up to date security patches and virus protection, and permission from their line manager; or
- provide unauthorised users with access to the EA network.

9. REMOVABLE MEDIA

The purpose of this policy is to protect the integrity of the data that resides within EA. This policy intends to:

- prevent data from being deliberately or inadvertently moved outside the EA network or physical premises where it can potentially be subject to unauthorised access; and
- prevent corruption or loss of data through malware introduced to the EA network by removable media.

This policy applies to the connection of removable media to any EA system or device within the EA network or related technology infrastructure. This removable media policy applies to, but is not limited to, all devices and accompanying media that fit the following device classifications:

- Portable USB-based memory pens, also known as flash drives, thumb drives, jump drives or key drives
- Memory cards in SD, CompactFlash, Memory Stick or any related flash-based storage media
- USB card readers that allow connectivity to a PC
- Portable MP3 and MPEG devices such as iPods with internal flash or hard-drive-based memory that support a data storage function
- Mobile phone handsets and smartphones with internal flash or hard-drive-based memory that support data storage function
- Digital cameras with internal or external memory support
- Removable memory-based media, such as writable DVDs, CDs and external hard-drives
- Any hardware that provides connectivity to USB devices through means such as wireless (WiFi, irDA, Bluetooth among others) or wired network access
- Tablets

This policy is complementary to any related policies dealing with data access, data storage or data movement.

9.1 Access Control

In order to preserve the integrity of organisational data and systems, EA reserves the right to prevent connection of unauthorised removable media devices to EA ICT facilities. This access control will be enforced through network policy and any other means EA deems appropriate to limit the ability of users to transfer data to and from ICT resources on the EA network.

9.2 What users MUST do

At all times users must:

- purchase all removable media through the central EA ICT procurement channel. The use of removable media obtained from any other source could present security and legal issues for EA, and as such is strictly prohibited. All newly purchased removable media devices will be delivered to EA ICT Services for registration and issue to users;
- apply approved secure data management procedures to the use of removable media, USB devices and related software for data storage, back up, transfer or any other action within EA's technology infrastructure;

- ensure that any portable memory used to conduct EA business is utilised appropriately, responsibly and ethically;
- employ reasonable physical security measures to secure all removable media devices whether or not they are actually in use;
- permanently erase data from removable media devices once their use by staff or contractors is no longer required; and
- immediately report any incident or suspected incident of unauthorised data access, data loss or disclosure.

9.3 What users must NOT do

At no time may users:

- connect any removable media device which has not been issued by EA ICT Services to the EA network infrastructure;
- use removable media to access, back up or store any enterprise-related data without authorisation;
- transfer sensitive or personal organisation data to authorised removable media unless the media contains EA security controls. Users should not transfer sensitive or personal data to removable media unless there is a compelling business requirement to do so.

9.4 Monitoring

EA will monitor the attachment of external devices to network resources and the resulting audit reports may be used for investigation of possible breaches or misuse of ICT resources. As a condition of use, users must agree to and accept that access or connection to the EA network may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. This is done in order to identify accounts or computers that may have been compromised. In all cases, the protection of individual and organisational data and systems is the purpose of such monitoring.

10. SOFTWARE USE

This document sets out the policy of EA in relation to software use, incorporating the acquisition, installation, licensing and disposal of all software made available to EA staff and contractors. This policy applies to all software managed, supported, owned or leased by EA.

The policy is designed to ensure:

- auditable compliance with regard to all software licenses
- suitable use of authorised software on all EA equipment
- reduction of risk against malware attacks

EA will supply users with appropriate software to assist with the duties associated with their role within the organisation. This will be done in accordance with the terms and conditions of individual license agreements. Users should be aware of the following to ensure legal compliance regarding the use of any software on EA equipment.

10.1 What users MUST do

At all times users must:

- purchase all software through the central EA ICT procurement channel. The use of software obtained from any other source could present security and legal issues for EA, and as such is strictly prohibited;
- ensure that all software products are used in accordance with software license agreements;
- inform EA ICT Services of all staff transfers so that the appropriate software can be added or removed and to ensure that all appropriate software and asset registers are updated; and
- store source software in secure locations and if deemed appropriate within fireproof safes.

10.2 What users must NOT do

At no time may users:

- make, acquire or use unauthorised copies of computer software or documentation;
- purchase software on behalf of the organisation, this includes the online purchase and downloading of software using means such as credit cards unless specifically approved by management;
- attempt to install unauthorised software or software upgrades. All software, unless otherwise specified, may only be installed by the EA ICT Services. All software updates will be carried out using centralised deployment tools, under the guidance of EA ICT Services;
- attempt to uninstall software or software upgrades. The removal of all software used by staff must be carried out by EA ICT Services to ensure that all appropriate software registers are updated; or
- download or install software from external sources. This includes software programs, instant messaging programs, screensavers, photos, video clips and music files.

10.3 Supply and Delivery

All newly purchased software will be delivered to EA ICT Services so that licences can be checked and recorded on the software asset register. In situations where purchased software has no physical delivery (such as software only available online) or for which only additional licenses are purchased, then all applicable licenses and paperwork must be delivered to EA ICT Services. No other user may take delivery of computer software.

10.4 Compliance

EA ICT Services will ensure license compliance via the use of software auditing tools. Users should be aware that there will be regular audits of software use to ensure compliance with external standards groups. EA ICT Services will also undertake random audits of any or all EA owned computer systems. Any software for which a valid license or proof of license cannot be determined or purchased will be removed.

10.5 Software licensing

All users must ensure compliance with legal restrictions on the use of material in respect of which there may be intellectual property rights, such as copyright, design rights, trademarks.

Unauthorised Copies

The unauthorised duplication of copyrighted software or documentation is a violation of the law and is contrary to established standards of conduct for employees. Members of staff who make, acquire or use unauthorised copies of computer software or documentation may be subject to disciplinary procedures. All software/information products must be used in accordance with software license agreements.

Additional Copies

In some cases, the license agreement for a particular software program may permit an additional copy to be placed on a portable computer or home computer provided only one user uses both installations. Users may not make such additional copies of software or documentation. All such requests must be forwarded to EA ICT Services who, after receiving approval that there are valid business reasons, will arrange for the installation of the additional copy.

11. REVIEW

This policy will be reviewed after two years with input from Trade Union side and other relevant stakeholders.

12. APPENDIX

Appendix 1 – Mobile Computing: Definition of Devices

Laptop/ Notebook	The general terms "laptop" or "notebook" can be used to refer to a number of classes of small portable computers.
Mobile Phone	In addition to the standard voice function, current phones may also support many additional services and accessories, such as SMS for text messaging, email, packet switching for access to the Internet, gaming, Bluetooth, infrared, camera with video recorder, MMS for sending and receiving photos and video, MP3 player, radio and GPS.
Smartphone	A smartphone is a mobile phone offering advanced capabilities beyond a typical mobile phone, often with PC-like functionality such as iPhone, Windows phone, Blackberry.
Tablet Computer	A mobile computer usually having a touchscreen or pen-enabled interface.