ICT Security Policy

This policy sets out to define the security controls for the use of ICT equipment and data.

Policy Number:	*5.12*	*Version number:*	*4*
Date of issue:	*15th August 2016*	*Date Archived:*	
Reason for policy: (Redraft)	*Redraft into CA Format*		
Authorised by: _____ ***On Behalf of Management***		*(Signature)*	
Agreed by: _____ ***UNISON Representative***		*(Signature)*	
Agreed by: _____ ***Unite Representative***		*(Signature)*	

N.B. The original copy of this policy containing signatures is held in the Human Resources office.

CONTENTS

1. Introduction

The objective of this policy is to provide management and employees direction for the protection of information owned by The Combined Authority and its customers, partners or suppliers, in whatever form it may be held or communicated, whether verbal, on paper or electronic. Information is one of our most valuable assets. Of equal value is the trust of our partners and customers that we will protect the information that they have shared with us.

The CA's proprietary, customer, partner and supplier information and data must be protected from unauthorised access, use, modification or destruction when it is created, stored, transmitted or communicated. Consequently, all access to, and use of, this information and data, requires adherence to the following policy principles:

- **Confidentiality** - Appropriate measures must be taken to ensure that the CA's information and data is only accessible to those who are authorised to have access to it.

- **Integrity** - The accuracy and completeness of the CA's information must be maintained and all changes or modifications affecting that information must be authorised, controlled, and validated.

- **Availability** – Information must be available to authorised individuals when required. In the event of a disaster or malicious attack, the CA's information and the systems critical to the success of our business must be recoverable.

- **Authentication** - All persons and systems seeking access to information or to our networked computer resources must first establish their identity to the CA's satisfaction.

- **Access Control** - The privilege to view, or modify information, computer programs, or the systems, on which the information resides, must be restricted to only those whose job functions absolutely require it.

- **Auditing** - User access and activity on the CA's computers, firewalls and networks must be recorded and maintained in compliance with all security, retention, and regulatory requirements.

Security policies and procedures are in place to support these objectives. The Head of ICT Services has responsibility for the maintenance of the security policies.

2. Policy Purpose

The purpose of this policy is to make everyone aware of their responsibilities to:

- Ensure that computer equipment is not subjected to hazardous conditions
- Ensure that systems and information are protected from unauthorised access
- Ensure the confidentiality of restricted information
- Ensure the correctness of information
- Meet the regulatory and legislative requirements in respect of information
- Assist in the production, maintenance and testing of business continuity plans
- Report any breaches of ICT security actual or suspected, to the ICT Service Desk.

The scope of this policy applies to ICT usage, including:

- Internet, CA email, CA applications and CA data which are accessed from using a device (desktop computer, laptop, tablet, mobile phone etc.) that is operated and utilised by the Combined Authority
- Internet, CA email, CA applications and CA data which are accessed from equipment which is not owned by the Combined Authority , but utilises the CA network or internet connection

3. Related Policies & Employment Legislation

- ICT Email and Internet Policy
- ICT Equipment Disposal and Returns Policy
- ICT Account and Password Policy

We remain up to date and compliant with all current employment legislation.

4. Our Responsibilities

4.1 Line Manager's Responsibilities

It is every Line Manager's responsibility to ensure that both they and members of their team within their line management responsibility comply with this policy.

4.2 Employee Responsibilities

It is the responsibility of every CA employee to ensure that they comply with and do not abuse the policy.

4.3 Information Asset Owners

In line with the Local Government guidelines an Information Asset Owner will be appointed for all systems that contain data that is covered by the Data Protection Act. The Information Asset Owner is the business manager who operationally owns the information contained in their system. Their role is to understand what information is held, how it is used and transferred, and who has access to it and why, in order for business to be transacted within an acceptable level of risk.

System	Software	Information Asset Owner
Human Resources	Carval	Head of HR
Payroll	Payrite	Head of Finance
Education Transport	CoSA	Lead Education Transport Co-ordinator
Customer Relationship Management (CRM)	MS Dynamics	Information and Marketing Manager
Complaints	MS Dynamics	Information and Marketing Manager
Travel centre Sales	Haven	Concessions & Integrated Ticketing Manager
Card Management	Innovator	Concessions & Integrated Ticketing Manager
Accessbus Booking	Data Images	Bus Services Manager
Procurement	Proactis	Head of Finance
Finance	Dream	Head of Finance
Bus services	CoSA	Bus Services Manager
On Street Infrastructure	CoSA	Facilities & Office Manager
Surveys and Reimbursement	CoSA	Bus Services Manager
Assets	Facility	Facilities & Office Manager
ICT Assets	Service Desk	Technical Services Manager

5. Procedure

5.1 Restricted Data

Restricted data includes personal data covered by the Data Protection Act 1998 as well as commercially sensitive or confidential data.

All employees have a common law duty of confidentiality in respect of information that arises from their contract of employment. Legal duties of confidentiality in respect of data relating to individuals also arise under the Data Protection Act 1998 (for more information on this see, the CA's Data Protection Code of Practice available on the Intranet

When considering what might be regarded as confidential, individuals should be particularly careful with:

- Matters relating to personnel or individuals,
- Commercially sensitive information regarding tenders and contracts or bus operators,
- Politically sensitive reports or information
- Any material that might undermine the CA or damage the CA's reputation.

A common sense approach should be adopted. If information is already in the public domain, e.g. it is on the external website, then no issues of confidentiality arise, but if in doubt about what information or data might be regarded as confidential, you must seek guidance from your Line Manager.

The transfer of restricted information over unprotected communication (such as a wireless network that does not have data encryption enabled) is not permitted. Where it is required to transfer restricted data from central storage systems, the data should be encrypted or transferred using the CA's, or an approved, secure file transfer protocol (ftp) site. It is not permitted to use laptops to view or process restricted information when in a public area.

5.2 Procedures

Authorisation to copy restricted data must be obtained from the Information Asset Owner. The request might be for a specific authorisation (for example - to copy a specific set of data on a particular day), a regular authorisation (for example - to copy a specific set of data once a month) or a more general authorisation. A record of all authorisations will be retained by the Information Asset Owner.

Transfer of restricted data will only be done using secure methods that have been approved by the ICT Management team. These will include but not limited to, the CA's secure ftp website, encrypted CD/DVD, encrypted USB memory stick, third party hosted storage that is encrypted and also provides encrypted transmission of the data. CD/DVDs and memory sticks are easily lost or stolen and must not be used for the storage or bulk transfer of personal data covered by the Data Protection Act.

Normal email systems are not secure and it is never acceptable to transfer bulk personal information via normal email services. Individuals should always contact the ICT Service

Desk over matters relating to the transfer (or emailing) of data which may be of a sensitive nature.

Where data covered by the Data Protection Act has been transferred to a third party the sender must check (and record) that the data has arrived.

The writing of data to CD/DVDs should be requested from the ICT Service Desk. Employees outside the ICT Service do not have the ability to create CD/DVDs. All requests for data to be written to CD/DVDs will be recorded in the ICT Service Desk System.

Where restricted data is to be copied on to or processed on a laptop, the laptop hard drive must be encrypted by ICT employees and recorded in the ICT Service Desk System.

The loss of a CD/DVD containing restricted data, a USB memory stick, or a laptop must be immediately reported to the ICT Service Desk.
Confidential data must not be copied into or stored in the Common file area or in any general Share area.

6. DESKTOP & LAPTOP COMPUTERS

6.1 Policy Statement

It is the responsibility of each user to take all reasonable precautions to safeguard the physical security of the computer. This includes protecting it from hazards, such as spilling liquids. It is also not permitted to connect personal USB drives to CA computers.

Users will be reminded of their extra responsibilities when they borrow a laptop computer to use either on the premises or away from the premises. Where restricted data is to be copied on to or processed on a laptop, the laptop hard drive must be encrypted.

6.2 Desktop Computers

Desktop computers must not be left logged in when unattended. If this is to be for a short time then users should lock the screen display using the CTL, ALT, DEL keys and clicking the “Lock Workstation” tab. If users fail to do this the desktop computer will automatically lock out after 15 minutes.

Information related to the CA’s business must always be stored on the central computer storage systems and not on the hard disk of the desktop computer.

6.3 Laptop Computers

Laptop computers must not be left logged in when unattended. If this is to be for a short time then users should lock the screen display using the CTL, ALT, DEL keys and clicking the “Lock Workstation” tab. If users fail to do this the laptop computer will automatically lock out after 15 minutes.

Laptop computers must never be left unattended, unless they are securely fastened by an anchor point. When not in use they must be stored out of sight.

It is only permitted to store restricted data on the hard drive of the laptop computer if it has been encrypted by ICT services.

When used in a public place it is not permitted to view or process restricted data. Care must be taken to ensure that the screen display cannot be overlooked when viewing or processing other data.

Laptop computers must never be left on view in a vehicle. They must always be stored in the boot. They must not be left in the vehicle overnight. Whilst in transit laptop computers should be placed in a suitable carrying case.

7. MOBILE PHONES, SMARTPHONES & TABLET PCS

7.1. Policy Statement

It is the responsibility of each user to take all reasonable precautions to safeguard the physical security of the equipment. This includes protecting it from theft. The equipment must only be used for the purposes for which it was provided.

7.2. Procedure

ICT will allocate equipment to individual members of staff following authorisation by the appropriate Head of Service or Director or as part of a team that needs them to carry out their role. ICT will retain a copy of the authorisation form where required and will maintain an inventory of all equipment and SIM cards. When the individual leaves the CA or moves to a role where the equipment is no longer required the equipment will be returned to the ICT Service Desk.

If the equipment is lost or stolen it must be reported to the ICT Service Desk as soon as possible. If the equipment contained confidential information, the ICT Service Desk will notify a member of the ICT Management Team. ICT Services will be responsible for remotely wiping any data stored on the equipment such as emails where possible. ICT Services will be responsible for ensuring that the SIM card is disabled and the phone is locked by the service provider.

It is not permitted to store confidential data on any of this equipment which is not protected by a complex password.

It is not permitted to connect this equipment to any personal equipment such as but not limited to home desktop computers and laptops – although connecting this equipment to Wi-Fi networks outside the CA is permitted.

When used in public places the user must take additional care. The equipment must not be left unattended where it can be easily stolen. Users must take care that the equipment

is not dropped or that liquids are spilt on them and should also avoid unauthorised people looking at the screen display.

The equipment must automatically lock following a period of 5 minutes inactivity. The user must then be forced to enter a personal identification number (PIN) or password to enable further use of the device. When the equipment is returned to ICT Services the PIN or password will be removed.

8. REMOVABLE DEVICES & MEDIA

8.1. Policy Statement

Only removable devices and media supplied by the CA or an approved source can be connected to CA computers. When holding restricted data the devices/media will be encrypted.

8.2. Procedure

Encrypted USB memory sticks can be allocated to individuals following authorisation by a member of the ICT Management Team. ICT will retain a copy of the authorisation form. your name will also be recorded against the asset in the ICT service management system. When you leave the CA or move to a post where an encrypted memory stick is not required the memory stick will be returned to ICT Services. Unencrypted memory sticks will only be issued in exceptional circumstances following authorisation by a Director.

The ICT Service Desk will maintain a record of users who have been allocated USB memory sticks. This will be audited on a periodic basis.

It is not permitted to store executable program files on these devices. Users will be reminded of their responsibilities when they are issued with a USB memory stick. The memory stick must always be removed from the computer when not in use and should be stored out of view.

The loss of any of the CA's USB memory sticks must be reported immediately to a member of the ICT Management Team.

Personal removable devices and memory sticks must not be connected to the CA's desktop or laptop computers. Such devices include, but are not limited to, USB memory sticks, external hard drives, CD/DVDs, digital cameras and mobile phones.

By default ICT Services will block all devices connected into the USB ports of the CA's desktop and laptop computers except for USB memory sticks issued by ICT Services, CA mobile phones and Blackberrys where there is a business reason for the connection and CA digital cameras or cards.

It is recognised that from time to time that it might be necessary to connect a memory stick from another organisation to a CA computer in a meeting room to load a presentation or file that is required for the meeting. The senior representative at the meeting must ensure that the representative of the external organisation is supervised.

USB memory sticks that are no longer required by an individual must be returned to ICT Services who will ensure that all data is removed before reuse or disposal. Appropriate records will be maintained.

9. NETWORKS

9.1. Policy Statement

There will be sufficient safeguards in place to prevent unauthorised persons from accessing the CA's IT systems. Where there is a need to connect with a third party's network or the public network a "firewall" will be installed.

9.2. Passwords

Access to ICT systems will require a password as well as the user identifier. These will need to be entered before accessing the CA's network and before accessing restricted systems, including applications, servers, and network devices.

Please see the ICT's Password Policy for details.

9.3. Managing Remote Access

All remote access to the CA's network will be through the Virtual Desktop Infrastructure (VDI), virtual private network (VPN), or through closed communication channels (point to point leased lines).

The CA's small remote offices and bus stations will be connected via dedicated MPLS lines, operated by Virgin Media under the YHPSN Framework.

All other CA users including home workers will be connected using either an approved VPN or via the VDI solution. Only CA owned PCs and laptops will be permitted to access the VPN and they will have firewall and antivirus software installed. Home or non-CA owned equipment may be used to access the VDI environment, but may be subject to restrictions or access denial if Operating Systems and antivirus systems are out of date.

Users from third parties who need to access the CA's network for support purposes must comply with the CA's Third Party Access Policy. Access will be supervised by ICT the team at all times.

Although access to systems managed and hosted by third parties is permitted outside the CA network, the issuing of user names and setting of permissions must be tightly controlled in order to provide limited and secure use.

10. PHYSICAL SECURITY

10.1. Policy Statement

The location of computer equipment will be planned taking into account the potential risks from fire, natural disasters and civil unrest. This will also take into account potential risks associated with neighbouring buildings.

10.2. Procedures

10.2.1. Electrical Protection

Key elements of the ICT systems will be protected against problems emanating from the power supply. These will include variations in power that may lead to failure in maintaining service and complete loss of power. All key systems, including servers and network equipment will be protected by an uninterruptible power supply.

10.2.2. Fire Protection

The main computer suite will be fitted with an automatic smoke detection system and an automatic fire suppression system. Appropriate fire extinguishers will be located immediately inside the access doors.

Flammable materials must not be stored inside the main computer suite.

10.2.3. Natural Disasters

Where possible, ICT installations will be located on a floor that is a reasonable distance above ground level to avoid flood damage. Installations should also avoid any internal plumbing systems.

10.2.4. Neighbouring Accommodation

Consideration will be given to the adjoining rooms and buildings when locating ICT installations. A risk analysis will be carried so that any risks can be mitigated.

10.2.5. Standby Services

Uninterruptible power supply systems will be provided to ensure that the service can maintained to enable ICT systems to be closed down in a controlled fashion.

11. Formal Action

Employees should note that any breaches of this policy may be considered either misconduct or gross misconduct and may lead to action within the CA's Disciplinary, Conduct & Capability Policy and Procedure. Serious breaches of this policy, for example incidents of bullying of colleagues or social media activity causing serious damage to the organisation, may constitute gross misconduct and lead to summary dismissal.

12. Equality Impact Assessment

In the creation of this policy, consideration has been given to any possible adverse equality impact for the following groups: disability; gender; gender reassignment; marital status (including civil partnerships); sexual orientation; race; religion or beliefs; age; pregnancy and maternity. The policy is considered to have little or no adverse equality impact.

13. Changes to Policy

The CA reserves the right to amend the details of this policy as required following consultation with recognised trade unions and other relevant parties.

This policy will be monitored and reviewed on an annual basis, to ensure that it meets the needs of the CA and ensure compliance with relevant legislation.

A written request can be made to review this policy at any time, by any of the signatories, giving appropriate reasons for requesting the review.