ICT Security Policy

ICT Services

January 2022

Contents

1. Introduction

The objective of this policy is to provide direction for the protection of systems and information owned by the Combined Authority, its customers, partners and suppliers. Of equal value is the trust of our partners and customers that we will protect any information which they share with us.

High standards of security is required to safeguard access to data and information at a systems level which involves the effective operation of firewalls, access rights and technical solutions. Equally importantly, data, information and assets must be physically protected to ensure that brute force cannot be used to obtain unauthorised access within the organisations buildings.

The Combined Authority'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 Combined Authority's information and data is only accessible to those who are authorised to have access to it.

- Integrity - The accuracy and completeness of the Combined Authority'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 Combined Authority'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 Combined Authority'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 Combined Authority'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 principles.

2. 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, information and physical assets 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.
- Securely store ICT equipment.

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

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

Unless stated otherwise, the policy applies to Combined Authority working locations and all other working environments such as homes, partner offices and public environments.

3. Related Policies

- Data Systems Security Incident Policy
- Email, Internet & Telecoms Usage Policy
- Equipment Allocation Policy
- ICT Equipment Display and Returns Policy
- Bring your Own Device (BYOD) Policy
- Password Policy

4. Our Responsibilities

Line Manager Responsibilities

It is every Line Manager’s responsibility to ensure that both they and members of their team within their line management responsibility have read this policy and are adhering to it.

Line Managers must inform the ICT Service Desk at least 5 working days before any end user who they are responsible for commences or ends their employment with the Combined Authority. Emails and personal data are retained for three months for all ex-employees unless the ICT Service Desk receives a line management request to vary this.

Employee Responsibilities

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

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 must also avoid unauthorised people looking at the screen display.

Information Asset Owners

As defined in the Data Protection & Confidentiality Policy, Information Asset Owners (IAO) are a Heads of Service (or Service Managers where no Head of Service is in place). IAOs must comply with the relevant Information Governance policies listed below:

- Data Protection & Confidentiality Policy
- Records Management and Data Quality Policy
- FOI-EIR Transparency Policy
- Data Security Incident Procedure

Human Resources

Human Resources must notify the ICT Service Desk within 24 hours of the effective time of a staffing change, which includes employment termination, new employment, suspension, or a change of job function (promotion, demotion, suspension, etc.). This includes all employment contracts issued by the organisation.

Similarly, accounts for contractors or temporary staff must be set up with an expiration date that is appropriate to the expected duration the account is required and in use. It is the responsibility of the recruiting manager to inform the ICT Service Desk of changes for individuals who are not employed by the Combined Authority.

5. Access to restricted data and copy/transfer activity

Restricted Data

All employees must be familiar with and comply with the relevant Information Governance and Data Protection policies listed in section 4 to understand what is classed as Restricted Data.

Access to Restricted Data

Access to data is controlled by the relevant Information Asset Owner (IAO) and requests must be sent to the ICT Service Desk, documenting a business reason, and signed off by the IAO.

ICT Services will only grant access to data with the authorisation of the IAO, or their nominated controller. Under exceptional circumstances, the IAO may grant access to a sensitive system or data to a user whose original role privileges may not have had such access before. This must be preceded by a documented business case Also, there might be need for an IAO at higher level to grant access to a user. This must only occur when there is a business critical need to access the data and the original IAO is not available to grant access. Irrespective of the business criticality of the request, every request must be logged with the ICT Service desk.

Copying or transferring Restricted Data

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 documented and retained by the Information Asset Owner.

Transfer of restricted data will only be done using secure methods that have been approved by ICT Services. These will include but not limited to:

- Microsoft OneDrive. This is suitable for sharing single files or folders with a limited number of internal or external parties. External file uploads are not permitted to OneDrive.
- Microsoft SharePoint. Where many files or folders need to be shared internally or externally with multiple people or organisations, a SharePoint site may be more appropriate. The relevant IAO can request the creation of a site via the ICT Service Desk. External file upload and collaboration may be allowed within SharePoint at the discretion of the IAO.
- Microsoft Teams. This is an internal sharing and collaboration tool, most suited for functional teams and projects. Team sites can be created by the appropriate IAO by submitting a request to the Marketing & Communications section.
- Other authorised file sharing platforms authorised by ICT Services and Legal & Governance Services.
- Encrypted CD/DVD/USB memory stick. Used for the physical transfer of data outside the Combined Authority.

Normal email systems are not secure, and it is never acceptable to transfer bulk personal information via normal email services. Transfer of data via email must always be encrypted. Individuals must 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 Regulations has been transferred to a third party the sender must check (and record) that the data has arrived.

The writing of data to removable media (including USB drives, CD/DVDs) should be requested from the ICT Service Desk. Employees outside ICT Services do not have the ability to create unencrypted copies of data on USB drives CDs and DVDs. All requests for data to be written to removable media 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 employees within ICT Services 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 using the dedicated ICT Security Incident template.

In the event of a lost data:

- This must be reported to the ICT service desk as per the methods shown on the Intranet (see ICT Services - Home (sharepoint.com))
- If the loss occurs within ICT Service Desk hours, the loss must be reported within 1 hour.
- Out of hours or during weekends, the loss must be reported the next working day.

Confidential data must not be copied into or stored in any common file locations such as Long/Short Term Share or SharePoint, Teams sites or other Office 365 locations which can be accessed by individuals not employed by the Combined Authority.

6. Laptop & Desktop Computers

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 or physical damage. It is not permitted to connect personal USB devices of any form to Combined Authority computers, unless for charging purposes. The ICT Services Team implement security Technical Security Measures to enforce this.

Laptop Computers

Users will be reminded of their extra responsibilities when they are issued with a laptop computer to use either on the premises or away from the premises. No laptop device is permitted to leave Combined Authority premises without full hard disk encryption.

Most Combined Authority users will be issued with laptop computers as standard. Laptop computers must not be left logged in when unattended. If the user is to be away from the device, even for short periods they must lock the screen display using the CTL+ALT+DEL keys and clicking the “Lock Workstation” tab or use the Windows Key + L key shortcut. If users fail to do this the laptop computer will automatically lock out after no more than 10 minutes

When used in the office, laptop computers must not be left unattended for extended periods or overnight. Also, in the office, secure desk locks are not available, but personal lockers are provided across office locations to securely store the laptops.

When a user is due to leave a Combined Authority building for any reason, even if the laptop is to be left in a secure locker, the Windows operating system must be properly shut down and not simply locked or set to sleep. When simply locked or set to sleep, the full disk encryption is less secure and could allow a stolen laptop to be accessed, therefore total shut down of the Windows operating system must be implemented.

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 must be placed in appropriate carrying case when transported.

Desktop Computers

Desktop computers must not be left logged in when unattended. If the user is to be away from the device, even for short periods they must lock the screen display using the CTL+ ALT+ DEL keys and clicking the “Lock Workstation” tab or use the Windows Key + L key shortcut.

7. Corporate Mobile Phones and Smartphones

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.

ICT Services will issue IT equipment to individuals as per the Equipment Allocation Procedure.

If an equipment used to access Combined Authority data and services is lost or stolen, it is the user’s responsibility to notify the ICT Service Desk as soon as possible via the incident template on the ICT Service Desk. Where necessary, 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 an appropriate password.

Where available, it is best practice to use face/fingerprint recognition and any other kind of biometric authentication systems must be implemented / enabled to access corporate data.

The equipment must automatically lock following a period of 5 minutes of 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.

No unauthorised applications must be installed on the device, via the Google Play Store or by any other method. If a new application is required, a request with associated business case can be submitted via the ICT Service Desk for approval.

8. Removable Devices & Media

Only removable devices and media supplied by the Combined Authority or an approved source can be connected to the organisation’s computers. When storing restricted data the devices/media will be encrypted.

Overnight storage of devices/media containing encrypted data must be within the locked Server Room with encryption keys only located in a private area of the company’s SharePoint system, encryption keys must never be stored with the associated devices/media.

Encrypted USB memory sticks can be allocated to individuals following authorisation by either the ICT Service Desk Co-ordinators or Technical Services Manager. Requests must be submitted via the ICT Service Desk and ICT Services will retain a copy of the authorisation. The name of the requester will be recorded against the asset in the ICT Service Desk system. When employees leave the employment of the Combined Authority or to a post where an encrypted memory stick is not required the memory stick will be returned to ICT Services.

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 must be stored out of view.

The loss of any of the Combined Authority’s USB memory sticks must be reported immediately via the ICT Service Desk using the ICT Security Incident template.

Personal removable devices and memory sticks must not be connected to the Combined Authority desktop or laptop computers to access data stored on them. 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 Combined Authority desktop and laptop computers except for USB memory sticks issued by ICT Services, mobile phones where there is a business reason for the connection and 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 Combined Authority computer in a meeting room to load a presentation or file that is required for the meeting. The senior representative at the meeting must arrange this via the ICT Service Desk and give reasonable notice. In this case, any non Combined Authority memory stick must be initially scanned for viruses before use.

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. The ICT service desk will maintain a list of staff issued memory sticks with their name and location. This list will be updated periodically to reflect the most recent status of the list.

9. Networks & Cyber Security

ICT Services will ensure sufficient safeguards are in place to prevent unauthorised persons from accessing the Combined Authority’s IT systems. It is the user’s responsibility to ensure the security of systems by ensuring their equipment and passwords are not compromised or accessible by malicious sources.

Where there is a need to connect with a third party’s network, a firewall or secure network connection will be used.

Passwords

Staff are to revert to the password policy for the purpose and approved standard for the creation of strong passwords and their protection.

The Combined Authority’s Password policy can be found on the intranet.

Managing Remote Access

All remote access to the Combined Authorities internal network will be through the virtual private network (VPN), or through closed communication channels (point to point leased lines).

The Combined Authorities small remote offices and bus stations will be connected via dedicated Multiprotocol Label Switching (MPLS) lines, operated by Virgin Media under the Yorkshire and Humber Public Services Network (YHPSN) Framework.

ICT services may restrict access to personal devices that exhibit unsecure behaviour such as out of date operating system or anti-virus.

The VPN solution is only available to corporate devices and will form a secure connection back to the Combined Authority network whenever an Internet connection is detected. Once connected to the VPN the device will appear as though it is physically located within the perimeter of a Combined Authority premise. No personal device will be permitted to access the VPN.

A large subset of Combined Authority data and systems can also be accessed via Microsoft 365 via the Internet. ICT services may restrict access to personal devices that exhibit unsecure behaviour such as out of date operating system or anti-virus.

Access to any Combined Authority systems by known 3rd parties should be requested via the ICT Service Desk to ensure due process is followed.

Cyber Security

All users must be familiar with basic Cyber Security principles which can be found in the mandatory training modules. As a Combined Authority employee, you have a duty to ensure the integrity of systems and data by remaining vigilant to threats and questioning when unsure. Users must be familiar with the main forms of Cyber Security threats including but not limited to:

- Social Engineering. Attackers use various methods to obtain credentials or information needed to gain access to systems. This could be via email, phone calls, social media or impersonating a trusted source.

- Phishing. The act of sending an email that looks to have come from a legitimate source, requesting information or asking for money to be transferred. It may appear to come from a trusted source, but usually contains demands or tight timescales designed to exert pressure.

- Malware. Any software or program designed to cause harm or exploit security flaws. It can take many forms, but the most common threat is Ransomware, designed to lock users out of files until a ransom payment is made. Malware may arrive though various methods, but the main method of distribution is via emails designed to look interesting or intriguing, enticing the user to open them. Malware may also be distributed via malicious websites using pop-ups.

Although Cyber Security threats can come in many forms and are sometimes very difficult to spot, users must remain vigilant and never open emails, click on links or visit websites that are sent by and unknown source.

If an employee is suspicious of any content or if it is thought they think they have detected a threat, this must be reported to the ICT Service Desk immediately.

10. Physical Security

The location of computer equipment will be planned in consideration of potential risks from fire, natural disasters and civil unrest. This will also consider potential risks associated with neighbouring buildings.

ICT Server Rooms and other ICT Areas

These are the responsibility of the Technical Services Manager.

The organisation's ICT Server Rooms and ICT Areas must be closed and locked at all times with restricted access limited to named individuals approved by the Technical Services Manager.

Visitor access should be recorded in a visitor log and entry to the ICT Server Rooms should be arranged and approved by one of the following who should accompany the visitor or arrange for a member of their team to do so:

- Technical Services Manager
- ICT Infrastructure Engineer
- ICT Service Desk Co-ordinator
- Head of ICT Services or above

Door locks used on ICT Server Rooms must be significantly more robust than the standard used by internal office locks used and able to withstand a level of physical force that is likely to be exerted by those seeking to unlawfully gain entry.

ICT Server Rooms must be neat, tidy with minimal dust. They should be highly clean environments with no rubbish, unkempt cabling and storage of items which are not essential to the provision of technology services. Food and drink is strictly not allowed in these areas.

Where room keys are used, these should either be combination locks or keys which are stored in a safe overnight. Combination lock codes used on Server Rooms, ICT Storage Areas or safes should be changed at least on a quarterly basis and these details recorded in a private SharePoint area. A strict key management procedure will be formulated and adhered to by all staff.

Safes used for ICT storage should be designed meet European standards for safes EN 1143-1:2015 grade 2 or higher.

Storage & Security of ICT Equipment

In order to securely store ICT equipment (mostly end user devices such as laptops and desktop PCs) a Storage Facility will be provided by Facilities and Assets. The integrity of this facility is the responsibility of Head of Assets while the Head of ICT Services is responsible for its management and operational use.

Access controls to the Storage Facility as well as protocols for the security of assets within the facility are set by the Head of ICT Services and Head of Assets or their delegated team members.

Volumes of storage and deliveries are managed by ICT Services and Facilities & Assets to ensure stock levels can be maintained within the facility.

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.

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.

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.

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.

Standby Services

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

11. System Permissions

All changes which affect access to data, network folders and system software must be logged with the ICT Service Desk.

- Changes must be logged by the Information Asset Owner of the resource in question.
- Where changes are required which will affect a person who is no longer employed by the Combined Authority, the request must be submitted by either:
    - The relevant Head-of service (if this person is of a higher grade than the ex-employee).
    - A member of the Senior Leadership Team (if this person is of a higher or equivalent grade than the ex-employee).
    - The appropriate Information Asset Owner
    - The Managing Director.

For information governance reasons, personal assistants and others cannot independently speak on behalf of more senior staff. Where necessary, required changes can be set-out by employees and forwarded to ictservicedesk@westyorks-ca.gov.uk by the Information Asset Owner or a Senior Leadership Team member with “approved” written next to the requirements.

12. 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 Combined Authority’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.

13. 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.

14. Changes to Policy

The Combined Authority 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 Combined Authority 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.

15. Accessibility

Accessibility has limited effect on this policy. All of the hardware, systems and software listed in this policy can be amended to suit accessibility needs to allow all users to comply. For end user devices e.g., laptops, special equipment can be provided to ensure accessibility is offered. Source policy documents are maintained in Word and stored in SharePoint Online, both of which have multiple accessibility options built in.