Information and Communications Technology (ICT) Usage Policy

Note: This document should be read in conjunction with the Code of Conduct, Data Protection, Data Retention Policy, Confidentiality Policies and Procedures within the Open Awards Staff Handbook

Contents

1 Introduction

Communications facilities are provided by Open Awards and made available to users for the purposes of the business. A certain amount of limited and responsible personal use by users is also permitted. All use of our communications facilities is governed by the terms of this policy, and if our rules and procedures are not adhered to, then use of our facilities may be curtailed or withdrawn, and disciplinary action may thereafter follow. Any breach of this policy may lead to disciplinary action being taken against you and serious breaches may lead to summary dismissal.

At Open Awards, communication plays an essential role in the conduct of our business. How you communicate with people not only reflects on you as an individual but also on us as an organisation. We value your ability to communicate with colleagues, clients/customers, and business contacts, and we invest substantially in information technology and communications systems which enable you to work more efficiently. We trust you to use them responsibly.

The general principles underlying all parts of this policy apply to email and internet facilities, use of computer applications and software, telephone communications, fax machines, copiers

and scanners. Note that some elements of personal use of Open Awards communications facilities are specifically addressed in this policy. Please read this policy carefully.

Open Awards Network
Open Awards servers are housed in the cloud and are patched and monitored by our external ICT support, with whom we are satisfied have robust contingency plans to meet our needs.

Whilst some aspects of IT administration are performed by named Open Awards staff (e.g., adding users, setting, and changing user access privileges, mailbox settings, installing approved software/applications), more technical functions and support is undertaken by our well-established, external IT support (MRD Technologies).

Their responsibilities include server and device monitoring, domain management, managed back-up service (detailed in the Disaster/Contingency Plan), network infrastructure, SonicWALL firewall and Sophos anti-virus, as well as general network support. Emails and data are located and backed up through the Microsoft 365 platform and data is recoverable through the Microsoft 365 recovery software. In addition, MRD also provide a managed backup service (M247) providing continuous synchronised backup to a network attached storage device located at MRD Technologies data Centre.

Open Awards database
Additionally, Open Awards utilises a web-based application, 'Quartz', created and hosted by Portico Consulting which support business management and operational process through a single integrated information system. These include built-in document management; built-in Microsoft Office integration; built-in CRM capability; and built-in support for key business processes including event management and provider approvals. Portico also operate a 'Helpdesk' for technical assistance and Change Requests. They are also responsible for ensuring Quartz data is backed up daily to two geographically separate locations.

Open Awards does not host the Quartz data servers.

Who does this policy apply to?

- This policy must be read and understood by all individuals working for Open Awards who use our Information and Communications Technology (ICT) facilities. This is all staff whether working remotely or on-site, trainees, contract staff, temporary and agency workers.
- Visitors to Open Awards premises and anyone using Open Award ICT resources will be made aware of ICT security arrangements.

Why have an acceptable use policy?

- It is important for us as an organisation to provide strict guidelines on the use of ICT resources. These guidelines help us to maintain the integrity of Open Awards and protect our members of staff.
- Acceptable use is defined as any use that supports Open Awards business and administrative activities and does not meet the definition of Prohibited Use.

How is it published & communicated to users?

- This policy forms part of the staff handbook, which is available in electronic format on the network, it also plays a role in the Induction Programme for New Starters.
- Changes or updates to the policy are communicated to staff through staff meetings and electronic notifications as and when required.

Disciplinary procedure

- Any member of staff not complying with this policy may face disciplinary action in accordance with the Open Awards 'Disciplinary Procedure' (see Staff Handbook)

2 General Computer Use

General Principles

You must use Open Awards Information and Communication Technology facilities sensibly, professionally, lawfully, and consistently with your duties, with respect for your colleagues and for Open Awards and in accordance with this policy and Open Awards other rules and procedures.

All information relating to our customers and our business operations is confidential. You must treat all paper-based and electronic information with utmost care and in accordance with the Clean Desk Policy (Appendix 1), Data Minimisation guidance (Appendix 2) of this policy and Data Protection Policy (Staff Handbook).

Many aspects of communication are protected by intellectual property rights which are infringed by copying. Downloading, uploading, posting, copying, possessing, processing, and distributing material from the internet may be an infringement of copyright or of other intellectual property rights.

Care must be taken when using email, Open Awards company blog or internal message boards as a means of communication. This is because all expressions of fact, intention and opinion in an email may bind you and/or Open Awards and can be produced in court in the same way as other kinds of written statements.

One of the advantages of using the internet and email is that they are extremely easy and informal ways of accessing and disseminating information, but this means that it is also easy to send out ill-considered statements. All messages sent on email systems or via the internet should demonstrate the same professionalism as that which would be taken when writing a letter or a fax. You must not use these media tools to do or say anything which would be subject to disciplinary or legal action in any other context such as sending any discriminatory (on the grounds of a person's sex, race, disability, age, sexual orientation, religion or belief), defamatory, or other unlawful material (for example, any material that is designed to be, or could be construed as, bullying or harassment by the recipient). If you are in doubt about a course of action, take advice from your line manager.

User Authentication

Azure Active Directory (Azure AD) system is the core user authentication system for the Open Awards network. Azure AD maintains lists of those who have access to the network

and Azure AD groups is used to grant privileged access to the network at a level deemed appropriate by Open Awards line managers and the ICT team.

Administrator access to the Azure AD system is strictly limited to named staff and our external ICT support, who work closely to maintain a current list of users and groups. Access privileges and permissions are limited only to that which an individual requires to carry out their job responsibilities and is reviewed by the ICT Technical Office (ICTO) and MIS and DATA Manager (MDM) at least twice a year.

Starter and leaver policies are in place that line managers complete to ensure staff entitled to access our data are given the right access privileges to perform their role, and no other access.

Privileged access

The creation of user accounts with higher privileges such as administrators is controlled and restricted to those users who have a clear business need to manage information systems or networks.

IT administrator accounts are strictly limited to named Open Awards staff and our external IT support. Administrator accounts are used for system administrative purposes only and do not have access to email, to mitigate the risk of malware spreading via privileged access. They are not used as standard user accounts.

Administrative roles are restricted to members of the Senior Management Team; the Head of Data, MIS and IT, and the ICT and Systems Technical Officer.

Installation of software and applications must be approved by the individual's line manager and implemented by an individual with an IT administrator account. Requests must identify a clear business need and outline levels of access required.

Technical support is sought from our external IT support as and when required.

An internal ICT ticket system is in operation for staff to request ICT related assistance.

User registration and deregistration

Initial user access is given only when the 'user' has been formally registered, and access permissions determined at an appropriate level, by way of the Starters and Leavers Policy and Open Awards ICT Access Management Record.

Guest accounts must be requested and authorised by a member of the Senior Manager Team (SMT). These accounts are more restrictive in nature but will also follow the same registration procedure as for new starters.

Where the IT and system access requirements of an individual change (for example, due to a change in responsibility or job role) the relevant line manager must submit an IT usage amendment request via the internal ICT ticket system so access can be removed from any functionality no longer required by the individual.

For security reasons it is essential that accounts are not left accessible for longer than is necessary once a member of staff is no longer employed by Open Awards. Accounts of leavers will be revoked, or login credentials changed with immediate effect, on the day their contract expires or by request on the instruction of the Line Manager or Director of Finance and Resources (DFR) (e.g., when an IT administrator leaves). Accounts may also be suspended/deactivated, on a temporary basis, on request of the CEO. In all instances, the 'Leavers Checklist' must be followed/completed by the ICT team to ensure nothing is overlooked.

After a period of 4 months the user accounts and mailbox of leavers will be deleted.

Usage

- Open Awards telephones, computers, laptops, tablets and printers and scanners are business resources and should not be used for personal activities without permission from a line manager.
- Do not dispose of any ICT equipment or data storage devices (e.g., USB or disc without prior approval from the ICT and Systems Technical Officer. Resources may contain commercial or personal sensitive data and require secure destruction.
- Each member of staff has a responsibility to use Open Awards equipment properly and take due care to prevent damage and only use it for its designated purpose. Any damage or loss of equipment or resources, including software and storage devices should be reported to the ICT and Systems Technical Officer immediately. If in doubt, speak to a member of the MIS, Data and ICT team.
- Any Health & Safety concerns regarding ICT equipment should be passed to the relevant line manager for attention as soon as possible. If in doubt, speak to a member of the MIS, Data and ICT team.
  Please take care when leaving drinks near electrical equipment and report any spillages immediately to your line manager or the ICT and Systems Technical Officer.

Data transfer between customers and Open Awards is primarily through the secure portal. Any sensitive files or data transferred via email or shared via SharePoint or Dropbox must be subject to appropriate security measures (such as file access restrictions, password protection or other encryption).

Data transfer to our regulators is through secure FTP sites with credentials unique to individual staff responsible for data uploads.

Prohibited use.

Prohibited use includes but is not limited to activity that:

- Staff are actively discouraged from using removable media (e.g., USB) and are encouraged to store data in the most appropriate location with security implications in mind. Use of removable media is currently prohibited but is under regular review.
- contravenes any laws, Open Awards policies or regulations or acts against Open Awards interests.
- involves the creation, downloading, storage or transmission of material that is indecent, offensive, defamatory, threatening, or discriminatory in nature. This includes pornography, hate speech, violence, and promotion of terrorism.

- involves threatening, abusive, obscene messages including those that may cause harm, offence, or harassment.
- harms Open Awards reputation or that of its staff.
- commits Open Awards to any contractual obligations without obtaining the appropriate authority.
- imitates or impersonates another person or their email address to create false accounts, send spam email or conduct any other activities unknown to the individual.
- introduces packet-sniffing or password-detecting software.
- intentionally or recklessly introduces any forms of spyware, computer virus or other potentially malicious software.
- constitutes a hacking activity.
- is undertaken for unauthorised, personal commercial gain.
- TikTok is prohibited on all company devices, to comply with the government controls.

Specifically, users are prohibited from:

- uninstalling any software, including anti-virus/malware, updates, or programs from Open Awards devices without permission from the ICT team.
- intentionally introducing any form of spyware or malicious software including computer viruses to the Open Awards network.
- sharing log-in credentials with another user.
- forwarding emails from a staff email account to a personal account.
- seeking to gain unauthorised access to restricted areas of the Open Awards network or knowingly accessing data which you know or ought to know is confidential or sensitive.

For your information, breach of a number of these items would not only contravene the terms of this policy but could in some circumstances also amount to the commission of an offence under the Computer Misuse Act 1990, which creates the following offences:

1. Unauthorised access to computer material i.e., hacking.
2. Unauthorised modification of computer material; and
3. Unauthorised access with intent to commit or facilitate the commission of further offences.

Software installation

- The installation of any software onto Open Awards computers/laptops is strictly prohibited (and enforced at user permission level) without permission from the ICT Technical Officer (ICTO). This is vital for the organisation to remain legally licensed for all our software and to ensure that computers/laptop performance and integrity of the Open Awards network and information systems are not adversely affected by non-essential or untested applications.
- The copying and/or installing of Open Awards software onto personal computers is also prohibited without prior permission from the ICT Technical Officer (ICTO) or Line Manager.

File management

- Each member of staff is allocated a personal storage space on the network (OneDrive) to keep their own files and folders. It is your responsibility to ensure that

any files saved to this area do not compromise the integrity of the organisation with any content derived from that defined in this policy as 'Prohibited Use'.

- Your personal OneDrive should not be used to store business critical or shared documents. Electronic documents of this nature should be stored in an appropriate shared location.
- All other areas of the network are strictly for business related files and folders only. Please ensure that these areas are used efficiently, and appropriate house-keeping measures are taken to keep files tidy and transparent for all users.

Fault reporting/support

- Any equipment or software faults on telephones, computers, laptops, and printers etc. or other support issues should be reported via the ICT Helpdesk. If you are unable to access the ICT Helpdesk, please speak to the ICT and Systems Technical Officer or your line manager who will take the appropriate action.

Disaster Recovery

- For information relating to disaster recovery in the event of an ICT failure, please see the 'Disaster/Contingency Plan' stored within the Staff Handbook.

Information Risk Management

To help protect our IT systems and data we:

- Ensure that computers, servers and remote access to all data is secure.
- Use anti-virus and anti-spyware protection, and enhanced firewalls.
- Regularly update software to the latest versions
- Check all are Cyber Essential certificated.
- Have secure backup systems in place.
- Ensure strong passwords are used and have 2-factor authentication in place.
- Train staff in IT policies and procedures.
- Have an Account Compromise Procedure in place (Appendix 3).

3 Email

Open Awards uses MS Outlook/Office 365 for all its email communications, this includes Microsoft 365 Message Encryption.

Work-related use

- You should always exercise extreme caution when opening emails from unknown external sources or where, for any reason, an email appears suspicious. The ICT Technical Officer should be informed immediately in such circumstances.
- If you open an email and are not sure of the integrity of the email content or sender, always contact the ICT Technical Officer for advice and do not open any file attachments under any circumstances. It is common for attachments to contain malware and spyware.
- Open Awards has an appropriate level of email security in place to identify and isolate undesirable emails. Those emails which are automatically moved to junk folders should be treated with great caution and only opened or 'whitelisted' if the user is confident of the senders' credentials.

- Staff are responsible for ensuring that unwanted items are deleted from their mailbox.
- Unwanted emails should be marked as junk/blacklisted as appropriate (antivirus and firewall protection is covered in the security section of this document)
- It is good practice to re-read and check an email before sending.
- Take care to check the appropriateness of copying the email addresses of other recipients into your email. You may be in breach of the Data Protection Act if it reveals other recipients' email addresses (e.g. in the case of marketing and mailing lists).

  Use the 'Bcc' (blind carbon copy) field instead of the 'Cc' (carbon copy) field when addressing an email to more than one recipient. If in doubt seek advice from your line manager.

  Please be aware of the 'Data Breach' procedures and follow these procedures should you be aware of data being shared with anyone it was not intended for.
- If the email message or attachment contains information which is time-critical, bear in mind that an email is not necessarily an instant communication and consider whether it is the most appropriate means of communication.
- If you have sent an important document, always request a read receipt and telephone to confirm that the email has been received and read.
- Customer related emails, including attachments, sent to or received from a customer should be moved to a shared location such as an appropriate area of the file directory structure or database. This constitutes good housekeeping practice and ensures that documents are readily accessible to those requiring access. This also applies to all internal email transmissions concerning customer matters. Refer to Appendix 2 Data Minimisation for guidance on saving documents containing personal information.
- Emails must not contain any personal and/or sensitive data unless the data is secured on an encrypted/password protected file. To do so would be to breach current data protection laws.

Personal use

Under no circumstances may Open Awards facilities be used in connection with the operation or management of any business other than that of Open Awards or a customer of Open Awards unless express permission has been obtained from your line manager.

- Email for personal activity is only allowed during your own time e.g., break & lunch times each day. Staff should use their own personal email account for non-business-related contact and must ensure that your personal email use: a) Does not interfere with the performance of your duties.
  b) Does not take priority over your work responsibilities.
  c) Is minimal and limited to taking place substantially outside of normal working hours (i.e. during any breaks which you are entitled to or before or after your normal hours of work);
  d) Does not cause unwarranted expense or liability to be incurred by Open. Awards.
  e) Does not have a negative impact on Open Awards in any way; and
  f) Is lawful and complies with this policy.
- All emails within your Open Awards mailbox folders, including your sent items are deemed to be business communications for the purpose of monitoring. By making

personal use of our facilities for sending and receiving email you signify your agreement to abide by the conditions imposed for their use and signify your consent to Open Awards monitoring your personal email.

Anti-social or unacceptable usage

- The passing on of chain mail, jokes, spam, animations, hoax virus warnings etc., is strictly prohibited.

Signature files

- Your signature file must follow the Open Awards corporate template signature containing your name, organisation, address, telephone, email, job role within Open Awards along with the company registration and charity numbers. A sample template signature file is available in the Corporate Branding Guidance in the Staff Handbook.
- Your signature should be listed on all business correspondence.

Attachments (sending & receiving)

- All attachments containing personal and/or sensitive data must be password protected.
- Passwords must be communicated to the recipient separately to the originating email. It is company policy that, where possible, personal and/or sensitive data should be transferred or exchanged through the Open Awards secure portal.

Viruses

- see *Security* Section

Mailbox management

Maintain good housekeeping by:

- Deleting any unwanted items from your mailbox folder.
- Aiming to keep the number of items in your inbox as low as possible by moving items you wish to retain to appropriate labelled folders and subfolders within your mailbox, Open Awards file structure or within Quartz as appropriate.
- Marking junk email as such and removing immediately.

4 Internet – Web and other online usage

We trust you to use the internet sensibly. Bear in mind always that, when visiting a website, information identifying your PC/Laptop may be logged. Therefore, any activity you engage in via the internet may affect Open Awards.

Work related use.

- All Open Awards staff have access to the internet for business use. Please close unused browser sessions to avoid stowing your active sessions and those of other users.
- Staff should be always vigilant.
- Pay particular attention to avoid downloading unwanted third-party spyware/malware/unwanted add-ons and other software.

Personal use

Open Awards recognises that users may make personal use of Open Awards systems, including email and internet, however personal usage must adhere to the following.

- Personal use should be reasonable and not excessive, ensuring that it does not interfere with IT resources, business requirements or any other Open Awards or legislative requirement.
- Personal use of Internet access is allowed during break & lunch times only.
- Explicit or offensive websites must not be visited, and any such abuse of your access privileges may result in disciplinary action. Open Awards reserves the right to monitor internet usage.
- You are strongly discouraged from providing your Open Awards email address when using public websites for non-business purposes. You should instead use your own, personal email account, e.g., Hotmail, Gmail etc for all non-business communications.

Downloading

- Downloading of large files such as music and video etc., are strictly prohibited without prior permission from the ICT Technical Officer or your Line Manager.

Offensive material

- You are responsible for the content of any material which is exposed to the office through email & web access etc. Offensive material is categorised as any item which may be deemed as offensive to others or inappropriate for the workplace. If you are unsure about which material can be classed as offensive, speak to a manager before you view it.

Messaging/chat

- The use of social media for personal use is only allowed during break & lunch times. Do not leave your account signed in outside of these times.

Online purchasing

- Staff that purchase goods online or view bank details etc., do so at their own risk, Open Awards will not be held responsible for any loss or theft resulting from personal internet access.

You must not use Open Awards systems to participate in any internet chat room or post messages on any external website, including any message boards or blog, unless expressly permitted in writing to do so by Open Awards.

5 Social Media

- Open Awards has a few social media accounts (Twitter, Facebook, Instagram, LinkedIn). When using the Open Awards social media accounts, you must follow the guidance provided in the social media – Acceptable Usage guidance and the Corporate Branding Guidance to ensure all posts fit within the ethos and business strategy of Open Awards. TikTok is prohibited on all company devices, to comply with the government controls. Care must be taken to ensure we do not breach any data protection laws (General Data Protection

Regulation 2018 – GDPR) in sharing any personal data unless explicit consent has been given and a record of this consent held by Open Awards as evidence. The Open Awards Data Protection Policy, available in the staff handbook, must be always adhered to.

6 Misuse of Facilities and Systems

Misuse of Open Awards telephone, email, and internet systems, in breach of this policy will be treated seriously and dealt with in accordance with Open Awards disciplinary procedure. Viewing, accessing, transmitting, posting, downloading, or uploading any of the following materials in the following ways, or using any of Open Award's facilities, will amount to gross misconduct capable or resulting in summary dismissal (this list is not exhaustive):

1. Material, which is sexist, racist, homophobic, xenophobic, pornographic, paedophilic, or similarly discriminatory and or/offensive.
2. Offensive, obscene, derogatory, or criminal material or material which is liable to cause embarrassment to Open Awards and any of its staff or its customers/clients or bring the reputation of Open Awards and any of its staff or its customers/clients into disrepute.
3. Any defamatory material about any person or organisation or material which includes statements which are untrue or of a deceptive nature.
4. Any material which, by intent or otherwise, harasses the recipient.
5. Any other statement which is designed to cause annoyance, inconvenience, or anxiety to anyone.
6. Any material which violates the privacy of others or unfairly criticises or misrepresents others.
7. Confidential information about (Open Awards) and any of its staff or customers/clients.
8. Material in breach of copyright and/or other intellectual property rights;
9. Online gambling; or
10. Unsolicited commercial or advertising material, chain letters or other junk mail of any kind.

If Open Awards has evidence of the examples of misuse set out above, or of a similar nature, it reserves the right to undertake a more detailed investigation in accordance with its disciplinary procedures.

7 Security

Security of our IT systems is of paramount importance. We owe a duty to all our customers/clients to ensure that all our business transactions are kept confidential and securely. If at any time we need to rely in court on any information which has been stored or processed using our IT systems, it is essential that we are able to demonstrate the integrity of those systems. Every time you use the system you take responsibility for the security implications of what you are doing.

General

- It is your responsibility to help always maintain the security of Open Awards ICT environment.
- All staff must ensure their own actions when using ICT resources, do not contribute towards any breach in security. Particular attention should be given to equipment and resources that are used off site such as laptops etc.
- Any visitors to the Open Awards office, who bring their own devices may be permitted to use the guest wireless network (password is stated on notices in training rooms). This is a restricted network and does not allow the user to access any part of the Open Awards network locations. If you identify any security risks that have not been addressed, please report them to the MIS, Data and ICT Team as soon as possible.
- Use the ICT Helpdesk system that is in place to ensure all reported incidents are recorded so they can be addressed immediately.
- Temporary staff will use 'guest/temp passwords' with restricted access to the Network.
- You should always exercise caution when opening emails from unknown external sources or where, for any reason, an email appears suspicious. The ICT Systems and Technical Officer should be informed immediately in such circumstances (see section 3 Email).
- On no account should anyone working for Open Awards attempt to access unauthorised or sensitive data and use this for personal use.
- **It is your utmost responsibility to notify the MIS Data, and ICT team immediately if you suspect that your network or email account has been compromised. If a member of the MIS, Data and ICT team is unavailable, then you should contact our external IT support for advice and assistance. Please see Appendix 3 Account Compromise Procedure for further details.**

Access and staff laptops

All staff use Open Awards laptops to access Open Awards data. Access is granted to staff after the 'Access Declaration' has been approved and signed. Access requires user login and password credentials and multi-factor authentication. All laptops are set up for staff use by the ICT Technical Officer and have BitLocker Drive Encryption switched on to protect our data from unauthorized access. Anti-virus software and an enhanced firewall is in place to manage/protect our network.

Access can and will be. Immediately revoked prevented if the need arises (e.g., account compromise) and at the request of the SMT.

Staff are instructed on safe remote-working and are subject to all aspects of the ICT Usage Policy whether they are working on or off-site.

- Open Awards staff are issued with a business laptop pre-installed with only the applications and software required to fulfil their Open Awards responsibilities, including anti-virus/malware software. Group-policies ensure that staff are actively prevented from installing software on their devices; this is only permittable at 'administrator' level, which is strictly restricted.
- Staff are required to sign an Access Declaration Form' before they are permitted to access Open Awards systems. The completed form should be returned to the ICT Technical Officer and signed copies are held in the MIS drive.

- Staff are also required to sign a ‘Laptop User Agreement’ form before taking their device off-site. This is managed by the ICT Technical Officer.
- Access to the network will time out after a period of inactivity.
- Laptops are monitored by our external IT support and includes regular patching as and when required.
- Staff must not print or copy sensitive data. This must be held in the relevant directory (see Appendix 2 Data minimisation).

When working off-site staff must:

1. Log onto the Open Awards remote connection to work.
2. Position themselves so that work cannot be seen by any other person (i.e. avoid ‘shoulder surfing’)
3. Lock their screen if they move away from their work area.
4. Take reasonable precautions to safeguard the security of Open Awards equipment,
5. Keep all passwords secure.
6. Inform the police and our ICT team or line manager as soon as possible if either their Open Awards laptop or computer equipment is lost or stolen.
7. Staff should also inform their line manager if personal equipment containing any Open Award related documentation/files is lost or stolen.
8. Ensure that any work is saved on the Open Awards network or is transferred to the Open Awards network as soon as reasonably practicable.
9. Report any security related notifications to the ICT team (e.g., anti-virus not updating).

All office procedures relating to ICT are still applicable when accessing the network remotely. Please familiarise yourself with this document thoroughly to help you understand your responsibilities.

Pocket computers, mobile phones and similar hand-held devices are easily lost or stolen so you must password-protect access to any such devices used by you on which is stored any personal data of which Open Awards is a data controller or any information relating to our business, our clients, or their business.

Data Protection

As a member of Open Awards who uses our communications facilities, you will inevitably be involved in processing personal and sensitive data for Open Awards as part of your job. Data protection is about the privacy of individuals and is governed by the Data Protection Act and General Data Protection Regulation 2018. This Act defines, among others, terms as follows:

1. "data" generally means information which is computerised or in a structured hard copy form.

2. "Personal data" is data which can identify someone, such as a name, a job title, a photograph.

3. "processing" is anything you do with data – just having data amounts to processing; and

4. "Data controller" is the person who controls the purposes and manner of processing of personal data – this will be Open Awards, in the case of personal data processed for the business.

- Open Awards must adhere to the requirements which are defined under the 'Data Protection Act and General Data Protection Regulation 2018.
- Additional information about our responsibilities is available at the Information Commissioner Office website https://ico.org.uk.
- Our data, especially learner information should be treated as sensitive in all cases and stored securely e.g., password protected/encrypted. Any paper records of sensitive data should be held securely until it can be disposed of and should then be disposed of securely using the locked confidential waste bins in the Open Awards office.
- Requests for access to data, i.e., a Subject Access Request (SAR) should be handled promptly and responsibly and in accordance with Open Awards procedures for dealing with SARs. Any issues or concerns should be raised with a manager prior to any information being released particularly in relation to any 3rd parties etc. (see Data Protection and Confidentiality Policies and Procedures).
- Keep all confidential information secure, use it only for the purposes intended and do not disclose it to any unauthorised third party.

Please refer to the Data Protection Policy contained in the Open Awards Staff Handbook for further information relating to Data Protection,

Passwords

- Keep your system passwords safe. Do not write passwords down or leave your workstation unlocked when away from your computer or laptop.
- Change your password every 4 months and use a combination of letters, numbers, and symbols to make your password as secure as possible.
- Always log out of systems when you are finished.
- Do not share your passwords with anyone.
- If a document is highly commercially confidential or price sensitive, you should mark it as "private and confidential" and password-protect the document itself. Bear in mind that documents which are NOT marked "private and confidential" can be accessed by all users of the network.

Password management

A useful technique for creating strong but memorable phrases is to pick three or four random words to form a long text string or a memorable sentence or phrase, ideally this should include punctuation and capitalisation.

Passwords should not be easy to guess for those who know or can research the individual e.g., family names, pets, birthdays, football teams or places.

An Account Compromise Procedure is in place in the event a user has any reason to believe that their password or account has been compromised. This must be used to immediately

alert the ICT team so immediate action can be taken to change the password to minimise any further risk to their account.

Staff who forget their password can request a re-set by contacting the ICT team. Accounts that have been automatically locked after too many attempts can also be unlocked by the ICT team. IT staff will only change a password and unlock an account once they are satisfied that the individual making the request is who they claim to be. Passwords are not to be re-used.

Service accounts should be set with strong passwords and changed immediately if they are believed to have been compromised. Default passwords for all systems and devices should be changed immediately.

The use of multi-factor has been rolled out to all staff and not just those where systems access represents a higher risk.

Back Ups

- Backups of our data is continuous for operational integrity.
- Files & folders can be restored through Microsoft 365. Should you need to retrieve a file or lost data, please speak to the ICT Technical Officer in the first instance who will guide you through restoring data to the required version. Have as much detail as possible about the file you wish to restore e.g., file name or keywords, file locations, date of last access of file to be restored.

Internet

- Open Awards use a security firewall to prevent unauthorised access to & from our site.
- This firewall also monitors internet and email access to help maintain the integrity of our organisation.
- You should not download or install software from external sources without having first received the necessary authorisation from the ICT Technical Officer or line manager.

Anti-virus/Malware

It is acknowledged that a high proportion of malware is a direct consequence of malicious emails and phishing attacks. This is addressed through this policy, staff training, communications, and induction.

- Only authorised anti-virus software may be used when connecting to the Open Awards network.
- You are responsible to ensure that every reasonable action has been taken, if you do contract a virus on Open Awards equipment.
- On-access scanning for both anti-virus and firewall is enabled on all devices. This is managed by our external ICT support.
- If you have any reason to believe they may not be running or up to date, then please contact the ICT team immediately for advice.

If you have any reason to suspect you have been a victim of any phishing attach or any other malware, please contact the ICT team immediately.

Network administration

- The ICT and Systems Technical Officer is responsible for the support of all Open Awards ICT equipment. Although we do use contractors for some areas of additional support, any problems should be reported in the first instance using the ICT Helpdesk system.
- Open Awards system or equipment must not be used in any way which may cause damage, or overloading or which may affect its performance or that of the internal or external network.
- No external device or equipment, including discs and other data storage devices, should be run on, or connected to Open Awards systems without the prior notification to and approval of the ICT and Systems Technical Officer or your line manager.

Mailboxes

User access to mailboxes and shared mailboxes is managed by the Database, MIS and ICT Manager following requests from line managers. User access to mailboxes, other than the users own, is granted on a need-to-know or business critical basis and is requested through the ICT Access Management Record.

Only IT Administrator accounts can make changes to mailbox settings which requires two factor authentication. This is managed by the ICT and Systems Technical Officer.

Quartz database

User access to the Open Awards database follows the principle of need-to-know and least privilege. Access control is managed locally and strictly limited to named members of the MIS, Data and ICT team.

Request for user access and changes to access (including downgrading or removal of access) must be made and agree through the ICT Access Management Record.

Quartz Portal

The Quartz portal is client-facing means of secure data transfer between customers and Open Awards. Only pre-approved users are provided with individual login credentials to the portal. Use of the portal is subject to the customer accepting the terms and conditions of usage and forbids the sharing of login credentials.

Passwords are to be changed at first login by a new user and password reset requests are automated. Permissions to use the portal are set at different levels in accordance with the customer role and privilege settings, regarding the role, are set and managed by the MIS, Data and ICT teambased on the business needs of the organisation (see Data Protection Policy). Privileges will be reviewed and changed as appropriate if the customer role changes.

Passwords may be revoked at any time if misuse or account compromise is suspected. The user accounts of customers who have no longer have a business relationship with Open Awards will be revoked.

8 Personal Blogs and Websites

This part of the policy and procedures applies to content that you publish on the internet (e.g., your contributions to blogs, message boards and social networking or content-sharing sites) even if created, updated, modified, or contributed to outside of working hours or when using personal IT systems.

Open Awards recognise that in your own private time you may wish to publish content on the internet. For the avoidance of doubt, such activities are expressly prohibited during work time or using Open Awards systems.

If you post any content to the internet, written, vocal or visual, which identifies, or could identify, you as a member of Open Awards staff and/or you discuss your work or anything related to Open Awards or its business, customers or staff, Open Awards expects you, at all times, to conduct yourself appropriately and in a manner which is consistent with your contract of employment and with Open Awards policies and procedures. It should be noted that simply revealing your name or a visual image of yourself could be sufficient to identify you as an individual who works for Open Awards.

If you already have a personal blog or website which indicates in any way that you work for Open Awards you should report this to your line manager.

If you intend to create a personal blog or website that will say that you work for Open Awards, or in any way could identify you as someone who works for Open Awards then you should report this to your line manager.

If a blog posting clearly identifies that you work for Open Awards and you express any idea or opinion, then you should add a disclaimer such as "these are my own personal views and not those of Open Awards".

The following matters will be treated as gross misconduct capable of resulting in summary dismissal (this list is not exhaustive): Refer to the social media Acceptable Usage guidance in the Staff Handbook for further information on posting information through social media.

1. Revealing confidential information about Open Awards in a personal online posting. This might include revealing information relating to Open Awards customers, business plans, policies, staff, financial information, or internal discussions. Consult your line manager if you are unclear about what might be confidential.

2. Criticising or embarrassing Open Awards, its customers, or its staff in a public forum (including any website). You should always respect the corporate reputation of Open Awards and the privacy and feelings of others. If you have a genuine complaint to make about a colleague or workplace matter the correct procedure is to raise a grievance using the Open Awards grievance procedure (See Grievance Policy in Staff Handbook).

3. Accessing or updating a personal blog or website from Open Awards computers or during work time.

If you think that something on a blog or a website could give rise to a conflict of interest and in particular concerns issues of impartiality or confidentiality required by your role, then this must be discussed with your line manager.

If someone from the media or press contacts, you about your online publications that relate to Open Awards you should talk to your line manager before responding.

Online publications which do not identify the author as a member of Open Awards staff and do not mention Open Awards and are purely concerned with personal matters will normally fall outside the scope of the Open Awards Information and Communications Technology policy.

9 Monitoring

Open Awards is ultimately responsible for all business communications but subject to that will, so far as possible and appropriate, respect your privacy and autonomy while working. Open Awards may monitor your business communications for reasons which include:

1. providing evidence of business transactions.
2. ensuring that Open Awards business procedures, policies and contracts with staff are adhered to.
3. complying with any legal obligations.
4. monitoring standards of service, staff performance, and for staff training.
5. preventing or detecting unauthorised use of Open Awards communications systems or criminal activities; and
6. maintaining the effective operation of Open Awards communications systems.

Open Awards will monitor telephone, email, and internet traffic data (i.e., sender, receiver, subject; non-business attachments to email, numbers called and duration of calls; domain names of websites visited, duration of visits, and files downloaded from the internet) at a network level (but covering both personal and business communications) for the purposes specified above. For the purposes of maintaining your own personal privacy, you need to be aware that such monitoring might reveal sensitive personal data about you. For example, if you regularly visit websites which detail the activities of a particular political party or religious group, then those visits might indicate your political opinions or religious beliefs. By carrying out such activities using Open Awards facilities you consent to our processing any sensitive personal data about you which may be revealed by such monitoring.

Sometimes it is necessary for Open Awards to access your business communications during your absence, such as when you are away because you are ill or while you are on holiday. Unless your mailbox settings are such that the individuals who need to do this already have permission to view your inbox, access will be granted only with the permission of a manager of Open Awards.

Any emails which are not stored in your "Personal" folder in your mailbox, and which are not marked PERSONAL in the subject heading will be treated, for the purpose of availability for monitoring, as business communications since we will have no way of knowing that they were intended to be personal. Therefore, you must set up a rule to automate the routing of personal email to your personal folder – ask the ICT team for guidance on how to do this. Furthermore, there is a risk that any person authorised to access your mailbox may have their own preview pane option as a default setting, which would reveal the content of any of your personal email not filed in your "Personal" folder, whether such email is marked PERSONAL. It is up to you to prevent the inadvertent disclosure of the content of personal email by filing your personal email in accordance with this policy. You are responsible to anybody outside Open Awards who sends to you, or receives from you, a personal email, for the consequences of any breach of their privacy which may be caused by your failure to file your personal email.

In certain very limited circumstances we may, subject to compliance with any legal requirements, access email marked PERSONAL. Examples are when we have reasonable suspicion that they may reveal evidence of unlawful activity, including instances where there may be a breach of a contract with Open Awards.

All incoming emails are scanned using virus-checking software. The software will also block unsolicited marketing email (spam) and email which have potentially inappropriate attachments. If there is a suspected virus in an email which has been sent to you, the sender will automatically be notified, and you will receive notice that the email is not going to be delivered to you because it may contain a virus.

Changes to access rights

Changing of roles internally may require changes to access control privileges and user requirements in line with our commitment to limiting access on a need-to-know basis. Requests for changes should be made using the ICT Access Management Record/new starters and application requests form.

The MIS, Data and ICT Manager will also review access rights twice a year to monitor that they are set at the right level including removing/adding to appropriate groups and mailboxes.

Standard user (i.e., non-IT admin) accounts are prevented from downloading, installing and un-installing software and applications including firewall and antivirus/malware software) and automatic updates. These functions can only be performed by an IT administrator.

Assets

Information assets are procured by either the MIS, Data and ICT team or external ICT support. Care is taken to ensure that devices and software procured are fit for purpose and meet the business needs of Open Awards.

An ICT asset list is maintained by the MIS, Data and ICT team and includes software licences and purchases. This team is responsible for ensuring that only licensed software is installed on devices. Software and applications that are outdated or no longer required will be removed from ICT devices.

Staff requiring access to a laptop or mobile phone are required to sign-up to the relevant device-specific agreement after confirmation form their line manager.

Devices will be checked by the MIS, Data and ICT team to ensure appropriate levels of security including passcodes, firewall and anti-virus are in place before issuing the device to staff.

10 Training

All staff need to be aware of their responsibilities both when managing information and staying secure online.

Induction
You will receive initial ICT training from the ICT and Systems Technical Officer as part of your induction. If you have not had this training, then please speak to the ICT and Systems Technical Officer as soon as possible as you are required to acknowledge that you have read and understood this policy.

Additional Training
The MIS, Data and ICT team are always available to provide advice and guidance as and when required, however updates and training will be provided at different points throughout the year to ensure staff continue to be fully compliant with their responsibilities regarding data protection and ICT security. Updates and training may take the form of on-site or on-line training sessions/webinars, induction for new staff, agenda items at staff meetings, email updates, staff alerts and changes to documentation.

However, if you require further training in any area of ICT then please raise this with your line manager at your next development review. If you feel that your training need is urgent and may affect your immediate performance within your job role, then speak to your line manager immediately. Advice on the appropriate training is available from the MIS, Data and ICT Team.

11 Compliance with this Policy

Failure to comply with this policy may result in disciplinary action being taken against you under Open Awards disciplinary procedures, which may include summary dismissal, and/or in the withdrawal of permission to use the company's equipment for personal purposes. If there is anything in this policy that you do not understand, please discuss it with your line manager.

Please note that the procedures and policies outlined in this policy, and in any related policy, may be reviewed or changed at any time. You will be alerted to important changes and the updated policy will be available in the Staff Handbook.

12 Declaration

It is important that you have read and understood this policy and speak to your line manager or the ICT Technical Officer should you have any questions.

You will be confirming you have read and understood this policy and agree to abide by the information outlined therein once you open the policy through your self-service dashboard in HR Works.

Appendix 1

Clean Desk Policy

1. Overview

1.1 The purpose for this policy is to establish a culture of security and trust for all employees at Open Awards. An effective clean desk working practice, involving the participation and support of all Open Awards employees, can greatly protect paper documents that contain sensitive information about our customers and staff, and is a key step to reducing the risk of a security breach.

1.2. All employees should familiarise themselves with the guidelines of this policy. This policy applies to staff working remotely and at the Open Awards office. See Appendix 1a for guidance on what constitutes personal data and where to store it.

1.3. For the purposes of this policy 'Clean desk' refers to your working area. This includes your home-working area, Open Awards office and visits and meetings away from the home working and Open Awards office environment.

2. Purpose

2.1. The purpose for this policy is to establish the minimum requirements for maintaining a 'clean desk', where personal/sensitive information about our employees, intellectual property and customers is secure in locked areas and out of site.

2.2. The main reasons for a clean desk policy are:

2.2.1. A clean desk can produce a positive image when customers and other visitors are on site.

2.2.2. It reduces the threat of a security breach as confidential information will be locked away when unattended.

2.2.3. Sensitive documents left out can be viewed, stolen, or copied by a malicious entity.

3. Responsibility

3.1. All staff and individuals contracted to work on behalf of Open Awards are subject to this policy.

3.2. This policy equally applies to staff working from home-office locations as well as staff working at the Open Awards office.

4. Policy

4.1. At known extended periods away from your working area, such as a lunch break or meeting, sensitive working papers are expected to be placed in a secure location (ideally locked drawers or cabinets).

4.2. At the end of the working day the employee is expected to tidy their desk and to lock away office papers containing personal or sensitive data.

4.3. Staff working remotely are expected to avoid printing personal or commercially sensitive documents. Any documents of this nature are to be securely locked away until they can be returned to the Open Awards office for secure destruction. There is an expectation that staff needing to print significant amounts of sensitive information will only do this at the Open Awards office. Speak to your line manager if you need further clarification of acceptable limits.

4.4. Computer/laptops screens must be screen-locked when not in use and powered down at the end of the workday. Care should be given when using devices used during meetings or public locations.

4.5. Keys used for access to secure areas at the Open Awards office (including cabinets and drawers) must not be left at an unattended desk and should be returned to the key cabinet.

4.6. Documents containing personal or commercially sensitive data must be retrieved from printers/photocopiers immediately (including home-office locations).

4.7. Whiteboards and flip charts must be erased of personal, sensitive, and intellectual data.

4.8. The confidential waste bins should be used to dispose of sensitive documents when they are no longer needed.

4.9. Lock away portable devices and mass storage devices such as laptops, mobile phones, tablets, USB, and external hard drives when not in use.

4.9.1. Staff are strongly advised to avoid using mass storage devices such as disks, USB, and external hard drives. If they are necessary, they should be treated as sensitive and secure them in a locked drawer.

5. Additional action

5.1. Allocate time in your calendar to clear away your working area and power down devices at the end of your working day, this applies whether you are working from home or from the Open Awards office.

5.2. Always completely clear away your workspace before leaving for longer periods of time.

5.3. If in doubt – throw it out.

5.3.1. If you are unsure of whether a **duplicate** piece of sensitive documentation should be kept – it will probably be better to place it in the confidential waste bins in the Open Awards office.

5.3.2. If you are working from home, unwanted sensitive documents should be securely stored until such time that you can return to the office and place in the confidential waste bins.

5.4. Scan documents and file them electronically on the network where possible.

6. Enforcement

6.1. Any employee found to have violated this policy may be subject to disciplinary action.

Appendix 1a

Clean desk – what to lock away!

Open Awards processes and stores a wealth of data, including both personal and sensitive data. It includes everything from learner data to payroll data, off-site staff visits/meeting dates to the details of a telephone enquiry on a post-it note and lots of things in between!

It's important to note that both personal and professional information is vulnerable. Whilst Open Awards clearly wants to protect its business interests and avoid risking a data breach, the safeguarding of staff is also important.

What is personal and sensitive data?

Personal data is data relating to an individual who is or can be identified directly or indirectly, either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller. It also includes any expression of opinion or intentions about the individual.

Sensitive personal data

This elates to information concerning a subject's racial or ethnic origin, political **opinions**, religious beliefs, trade union activities, physical or mental health, sexual life, or details of criminal offences.

How to achieve a clean desk policy? Simply put….

PLAN

Keep out just the things you need for the workday on your desk – i.e., keep unnecessary files and folders locked away.

PROTECT information when you leave your work area.
Obviously, you will leave your desk numerous times during the working day. Before you do, make a quick check to see if there is sensitive information on your desk and place it in a folder or lock your screen i.e., out of sight.

PICK up at the end of the day.
Before you leave your desk for the day, ensure you put your paper documents away securely. Plus, there are productivity benefits with a clean desk first thing in the morning!

What should be stored securely?

Think damage limitation! Any items with personal/sensitive information relating to 'subjects' (i.e., people).
Examples include.

- Notepads
- Any paper notes (incl. scraps of paper) with personal details – including details taken by phone etc. – And notes on subjects.
- Diaries or information identifying location of a member of staff, time/date.
- Reports, registration data, achievement data (unless anonymised aggregated data)
- Contracts, staff records, name, and address/tel/email
- Payroll information and possibly invoices if using personal details, including banking details.
- Portable ICT equipment (phones, tablet, laptop, external storage – e.g., hard drives, USB, disk).
- Samples of work as these may contain details that could identify an individual.
- Attendance lists for events/training.
- Banking details
- Any document containing a ULN or Learner ID or name: this data doesn't necessarily have to have a further identifying factor with it (e.g., postcode, Provider, course, achievement/grade, ethnicity, disability, DOB) as further details may be easily obtainable separately. Best practice is to always secure anything with a ULN, Learner ID or name.

Where?

- Lockable desk drawers or cabinet at the Open Awards Office (let your line manager know if your office drawer does not have a key).
- Scan paper documents and store in a suitable network location (not your desktop)
- ICT equipment should be stored in the comms room, out of sight (i.e., in one of the cabinets) or stored away from view when at home.
- For further details and guidance of what and where to store documents and emails, please refer to the 'Data Minimisation' document (Appendix 2).

Appendix 2

Data minimisation

What is data minimisation?

Data Minimisation is an important **principle** of the GDPR which states that **data** collected and processed should not be held or further used unless this is essential for reasons that were clearly stated in advance to support **data** privacy.

In practical terms this is reinforcement that good house-keeping practices, *irrespective of GDPR*, must be adopted regarding data collection, storage and usage. This extends not only to data processed through Quartz, but any electronic files – i.e., emails and attachments, files and folders on PCs and the Open Awards network.

Purpose
The underlying principles are to protect and limit customer and staff data/information, collecting and storing only what is relevant, adequate, and necessary for the business – i.e., good quality information. Where this concerns personal data, it must also be with the data subject(s) explicit consent and necessary for carrying out the purpose for which the **data** is processed.

Open Awards therefore require all staff to review their own emails and attachments (inboxes, folders, sent items), electronic files and paper-based documents and continue to adopt this principle, with the purpose of retaining and processing only if they are business essential, are in accordance with our own Data Retention Policy and meet the Data Privacy requirements of the GDPR.

The benefits of acting include improving efficiency and transparency (easy to locate and access), facilitate response to Subject Access Requests, audits, decrease mail storage requirements, avoiding duplication and demonstrate Opens Awards commitment to fulfilling the legal requirements of the GDPR.

Action required.

Emails

- move emails/attachments to an appropriate ‘documents tab’ location in **Quartz** (see table A below) using the correct document ‘type’.
- move emails attachments to an appropriate location in a **network folder** as appropriate (see table below)
- delete emails that are no longer necessary e.g., emails moved to quartz, that are no longer required, information emailed to yourself • retain emails of a specific nature that don’t need to be shared but are required e.g.
  holidays, general queries, and conversations between staff.

Files

- store as anonymised data if personal data is not necessary (supports the general data minimisation approach)
- do not retain when they are no longer required (identified through periodic review)
- do not store on a OneDrive, PC desktop, portable storage device (e.g., USB) • avoid duplicating/holding in multiple locations.
- passwords protect or store in pre-agreed restricted folders if the contents are of a confidential nature (speak to ICTO if you need assistance with this)

Table A: Sample location for different email/files Category	**Location**	**Example**
Individual learner	Quartz – learner documents tab, with appropriate doc 'type;	Query regarding learner achievement
Course run/ group of learners on a particular run	Quartz – course run documents tab with appropriate doc 'type;	Malpractice on a particular run
Organisation	Quartz – organisation documents tab with appropriate doc 'type;	Maladministration at a centre
Data sharing partners (e.g. OfQual, ESFA, QAA, UCAS.XAMS etc)	Appropriate network folder, restricted to staff as appropriate (may be password protected)	ESFA data held on a restricted drive, with a data retention policy.
Finance		Finance drive, restricted to Finance team
Generic communications/files Assessments and evidence files	Shared generic folder on Open Awards share-point (or a broad heading for a specific business area if required) with appropriately named subfolders. Share-point – quality folder.	Marketing folder or Access to HE folder and associated sub-folders on Open. Awards share-point.

Practical suggestions:

- Use a 'holding file' for emails/files you identify need to be moved.
- - Emails should be stored with the full email thread, to avoid multiple versions of the communication (you may find this easier to do in Office 365)
- Use a temporary 'holding file' for emails you think you need to delete, and review this after a couple of weeks.
- Set up an email deletion rule (e.g., to delete mail in your 'Deleted Items' after 2 weeks)
- You may wish to target emails with attachments first as these are more likely to contain data.

- Set some time aside each day/week, for the initial clean up, so that it does not become one onerous task, and tackle one folder at a time.
- Make sure you maintain good practice moving forward!

Appendix 3

Account Compromise Procedure

Users must notify the MIS, Data and ICT team immediately if they suspect that their network or email account has been compromised/ hacked (or external IT support e.g. MRD Technologies helpdesk support@mrdtechnologies.co.uk if ICT team unavailable).

A user may also find they are locked out of their account, or there are messages sent from their account that they do not recognise. These are good indications that their account has been hacked or something has gone wrong.

In the event of any of the above occurring, the following procedure is to be followed:

1. The account must be checked to confirm that no unwanted email forwarding rules or filters are in place. This is a known trick used by hackers to send a copy of all your emails to them.
2. Check for any emails sent from the account that the user did not send.
3. The password for the account and network password is to be changed immediately (and all accounts that have the same password as the hacked account).
4. Operating Systems and apps on the PC's/laptops you use should all be updated with the latest security fixes.
5. Run a Sophos antivirus software scan and Malware Bytes scan on PC's and laptops (not usually necessary for phones and tablets).
6. Follow any other advice and guidance that the ICT/external IT support provide.

Please note that password reset links are not sent to staff. Resets are managed by the Data, MIS and ICT team and the user.

Notify your contacts.

The account owner should inform their contacts that they have been hacked, to help contacts avoid being hacked themselves. You should contact the people you know regardless of whether you managed to restore your account or not.

2-factor authentication

This has been rolled out to all staff and provides an extra layer of protection to 365 account users. 2-factor authentication requires that users verify access to their account through another method e.g., a verification message to the users' phone.

If you cannot recover your account, then you will likely need a new account setting up via the ICT team/external IT support. You should advise your contacts and update any sites with your new details (e.g., secure logins to QAA, OfQual etc).