Data and Information Security Policy

Contents

Policy Statement

Orangebox Training is committed to a policy of protecting the rights and privacy of individuals (includes learners, staff and other stakeholders) in accordance the General Data Protection Regulations (GDPR).

Orangebox Training needs to process certain information about its staff, learners and other individuals it has dealings with for administrative purposes (e.g. to recruit and pay staff, to administer programmes of learning, to record progress, to agree awards, to collect fees, and to comply with legal obligations to funding bodies and government). To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

This policy applies to all staff and learners of Orangebox Training. Any breach of the Data Protection Act 2018 (GDPR) is considered to be an offence and in that event, Orangebox Training disciplinary procedures will apply. As a matter of good practice, other agencies and individuals working with Orangebox Training, and who have access to personal information, will be expected to have read and comply with this policy. It is expected that departments/sections who deal with external agencies will take responsibility for ensuring that such agencies sign a contract agreeing to abide by this policy.

The purpose of this policy is to identify, assess, and appropriately mitigate vulnerabilities and threats to Orangebox Training which through the loss, corruption of or unauthorised access to critical information could adversely impact the critical business assets of the organisation. This includes ensuring business continuity and minimising business damage by preventing, detecting and responding to information security incidents and managing information security risks.

Orangebox Training Information Security Policy ensures that:

- Confidentiality of Orangebox Training information assets is maintained
- Integrity and authenticity of information is maintained
- Availability and usability of information is maintained
- Information is protected against unauthorised access
- Authentication is appropriately applied to validate user identities
- Contractual, Regulatory and Legislative Information Security requirements are met
- Business Continuity and risk management plans are produced, maintained and tested
- Change management is applied to maintain security
- Information security awareness training is available to all staff
- All security breaches, actual or suspected, are reported and investigated and action taken to improve procedures where required
- Information Security Policies, Procedures and Guidelines are documented and implemented to support this policy
- All information assets will be subject to formal risk assessment and treatment
- The Security Policy and the supporting policy documents are reviewed at least annually by the Data Controller and the Senior Management Team.

Data Protection Act 2018

The Data Protection Act 2018 enhances and broadens the scope of the Data.

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulations (GDPR).

The Data Protection Act 2018 controls how your personal information is used by organisations, businesses or the government.

There are separate safeguards for personal data relating to criminal convictions and offences.

Personal Data

S identified as data relating to a living individual who can be identified from that information or from that data and other information in possession of the data controller. It includes the name, address, telephone number, ID number. It also includes the expression of opinion about the individual, and of the intentions of the data controller in respect of that individual.

Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

Sensitive Data

There is stronger legal protection for more sensitive information, such as:

- race
- ethnic background
- political opinions
- religious beliefs
- trade union membership
- genetics
- biometrics (where used for identification)
- health
- sex life or orientation.

Data Controller

Any person (or organisation) who makes decisions with regard to particular personal data, including decisions regarding the purposes for which personal data are processed and the way in which the personal data are processed.

Data Subject

Any living individual who is the subject of personal data held by an organisation.

Processing

Any operation related to organisation, retrieval, disclosure and deletion of data including:

- Obtaining and recording data
- Accessing, altering, adding to, merging, deleting data
- Retrieval, consultation or use of data
- Disclosure or otherwise making available of data.

Third Party

Any individual/organisation other than the data subject, the data controller or its agents.

Relevant Filing System

This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

Please note that this is the definition of 'Relevant Filing System' in the Act. Personal data as defined, and covered, by the Act can be held in any format, electronic (including websites and emails), paper-based, photographic etc. from which the individual's information can be readily extracted.

Responsibilities under the Data Protection Act 2018 (GDPR)

System owners are responsible for submitting system change requests to the ICT support organisation using the change request form.

The following changes are considered routine or insignificant and are therefore not subject to this policy:

- Anti-virus updates
- Routine vendor issued patches to Windows operating systems and system software
- Vendor issued application patches.

All change requests will be subject to review by the ICT support company and the Data Controller to ensure the proposal remains in line with company policy. The Data Controller will consider the impacts upon Information Security and Business Continuity when undertaking the review.

Subject to a satisfactory review request will be formally authorised. Changes which are not authorised will not be made.

All changes will be subject to rigorous testing prior to deployment and will include suitable back out plans.

Emergency changes can be deployed without going through the associated Change Control Procedure however such emergency changes must be authorised by the Board and the Data Controller.

Emergency changes must be fully documented following the change with a clear explanation for the change and the reasoning as to why such a change was required in an emergency.

In all circumstances, only the asset owner can authorise the transfer of their system from the test environment to the operational (live) environment.

All staff are responsible for ensuring that any personal data (on others) which they hold is kept securely and that they are not disclosed to any unauthorised third party. All personal data should be accessible only to those who need to use it. You should form judgement based upon the sensitivity and value of the information in question, but always consider keeping personal data:

- Stored on Orangebox Trainings SharePoint or OneDrive cloud storage and data files password protected.
- In a lockable room with controlled access, or
- In a locked drawer or filing cabinet, or
- If computerised, password protected, or
- Kept on disks which are themselves kept securely.

Care should be taken to ensure that PCs and terminals are not visible except to authorised staff and that computer passwords are kept confidential. PC screens should not be left unattended without password protected screensavers and manual records should not be left where they can be accessed by unauthorised personnel.

Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data. Manual records should be shredded or disposed of as "confidential waste". Hard drives of redundant PCs should be wiped clean before disposal.

This policy also applies to staff and learners who process personal data "off-site". Offsite processing presents a potentially greater risk of loss, theft or damage to personal data. Staff and learners should take particular care when processing personal data at home or in other locations outside Orangebox Training.

Rights of Access to Data

To ensure that access to all Orangebox Training Information Systems is controlled with access being granted only to those who have a need to access specific information/systems. A failure to control access could allow unauthorised individuals or groups access to confidential information.

The company controls access to information on the basis of statutory, contractual, business and security requirements.

Access control rules and rights to applications, expressed in standard user profiles, for each user or group of users will be clearly stated, together with the business requirements met by the controls.

The security requirements of each business application are determined by a risk assessment that identifies all information related to the application and the risks to that information.

The access rights to each application will take into account:

- The classification levels of information processed within that application and ensure that there is consistency between the classification levels and access control requirements across the systems
- Data protection and privacy legislation and supplier contractual commitments regarding access to data or services
- The 'need to know' principle (i.e. access is granted at the minimum level necessary for the role)
- "Everything is generally forbidden unless expressly permitted"
- Rules that must always be enforced and those that are only guidelines,
- Prohibit, by restricting access to admin functionality, user-initiated changes to information labels
- Prohibit unauthorised changes to user permissions
- Enforcing, using up policies and application functionality, rules that require specific permission before enactment
- Any privileges that users actually need to perform their roles, subject to it.

The company has standard user access profiles for specific system and organisational roles in the business which share common resource requirements.

Management of access rights across the network is managed by the external IT support organisation.

User access requests, authorisation and administration will be segregated.

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the entire Orangebox Training network. Consequently, all employees (including contractors and vendors with access to Orangebox Training Systems) are to comply with Orangebox Training password procedures, as outlined in the following paragraphs, when selecting and securing passwords.

Orangebox Training Company password procedures is as follows:

- Passwords are to be at least 8 characters in length
- Passwords are to include upper and lowercase letters, numbers and special/punctuation characters (using at least 3 of the 4-character types listed)
- Passwords must be changed when prompted, or immediately where compromise is suspected
- Passwords issued to new users and other temporary/reset passwords provided by Orangebox Training Data Controller or ICT support organisation must be changed immediately after first use/logon

- Passwords must not be re-used/recycled
- Group passwords are not to be used
- User accounts will be locked out after 5 failed logon attempts
- The IT support organization will ensure that pre-set Vendor/Default passwords are changed prior to systems/assets being taken into use
- All network/system level passwords (including switches, firewalls, servers etc) are to be changed on termination/departure or change of IT support organisation.

Passwords must **not** be:

- shared with others*
- written down or stored on-line
- based on personal information, names of family
- a dictionary word (any language), slang, dialect, jargon etc.

*Not sharing passwords with others includes IT support staff, line managers or others claiming they need to know it for Company/technical/official purposes. If pressed refer demander to this policy.

This password procedure is to be applied to all Orangebox Training systems except where individual bespoke applications/systems are incompatible

Password Advice

Although Company policy requires a minimum of only 8 characters, the use of longer passwords is encouraged where systems permit; the longer the password, the more secure it is likely to be.

A suggestion is to take all or part of a sentence, saying, phrase etc and abbreviate it e.g.:

- IhwaIf2y (I have worked at Intartic for two years)
- Bitsumro6t9 (Back in the summer of sixty-nine)
- mt4ceBwu (May the force be with you).

Users are strongly encouraged to make use of such passwords as they can be easy to remember and virtually impossible to guess.

Passwords are considered to be weak if:

- The password is a word found in a dictionary
- The password is a common usage word such as: Names of family, pets, friends, co-workers, fantasy characters, etc. Computer terms, names, commands, sites, hardware, software. Personal information such as birthdays, addresses, phone number Word or number patterns
- Any of the above spelled backwards. Any of the above preceded or followed by a digit (e.g. secret1, 1secret).

Misuse

Improper use of passwords is to be reported immediately to the Data Controller and senior management.

Subject Access Request

Members of Orangebox Training have the right to access any personal data which is held by Orangebox Training in electronic format and manual records which form part of a relevant filing system. This includes the right to inspect confidential personal references received by Orangebox Training about that person.

Any individual who wishes to exercise this right should apply in writing to the Data Controller. Orangebox Training will not charge for complying with a subject access request but reserves the right to charge a fee for data subject access requests that are manifestly unfounded or excessive (currently £10). Any such request will normally be complied with within 1 month of receipt of the written request and, where appropriate, the fee. For information on responding to subject access requests see Appendix A of this policy.

In order to respond efficiently to subject access requests, Orangebox Training needs to have in place appropriate records management practices. See Appendices for further information on records management.

Disclosure of Data

Orangebox Training must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All staff and learners should exercise caution when asked to disclose personal data held on another individual to a third party. For instance, it would usually be deemed appropriate to disclose a colleague's work contact details in response to an enquiry regarding a particular function for which they are responsible. However, it would not be appropriate to disclose a colleague's work details to someone who wished to contact them regarding a nonwork-related matter. The important thing to bear in mind is whether or not disclosure of the information is relevant to, and necessary for, the conduct of business. Best practice, however, would be to take the contact details of the person making the enquiry and pass them onto the member of Orangebox Training concerned.

This policy determines that personal data may be legitimately disclosed where one of the following conditions apply:

- the individual has given their consent (e.g. a learner/member of staff has consented to Orangebox Training corresponding with a named third party)
- where the disclosure is in the legitimate interests of the institution (e.g. disclosure to staff - personal information can be disclosed to other employees if it is clear that those members of staff require the information to enable them to perform their jobs)
- where the institution is legally obliged to disclose the data (e.g. HESA and HESES returns, ethnic minority and disability monitoring)
- Where disclosure of data is required for the performance of a contract as long as such contract adheres to the current Data Protection Act.

When members of staff receive enquiries as to whether a named individual is a member of Orangebox Training, the enquirer should be asked why the information is required. If consent for disclosure has not been given and the reason is not one detailed above (i.e. consent not required), the member of staff should decline to comment. Even confirming whether or not an individual is a member of Orangebox Training may constitute an unauthorised disclosure.

Unless consent has been obtained from the data subject, information should not be disclosed over the telephone. Instead, the enquirer should be asked to provide documentary evidence to support their request. Ideally a statement from the data subject consenting to disclosure to the third party should accompany the request.

As an alternative to disclosing personal data, Orangebox Training may offer to do one of the following:

- Pass a message to the data subject asking them to contact the enquirer
- Accept a sealed envelope/incoming email message and attempt to forward it to the data subject.

Please remember to inform the enquirer that such action will be taken conditionally: i.e. "if the person is a member of Orangebox Training to avoid confirming their membership of, their presence in or their absence from, the organisation.

Retention and Disposal of Data

Records are defined as all those documents, which facilitate the business carried out by the company (to provide services to customers and learners) and which are thereafter retained (for a set period) or are used in the day to day running of the company. These records may be created, received or maintained in hard copy or electronic format.

This applies to all records created, received or maintained by staff of the company in the course of carrying out their daily duties.

Records management is defined as a field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of, and information about, business activities and transactions.

The company has a corporate responsibility to maintain its records and recordkeeping systems in accordance with the regulatory environment. The role with overall responsibility for this policy is the MD.

The Data Controller is responsible for drawing up guidance for good records management practice and promoting compliance with this policy in such a way as to ensure the easy, appropriate and timely retrieval of information.

Individual employees must ensure that records for which they are responsible are accurate, and are maintained and disposed of in accordance with the company's records management guidelines.

The destruction of records will only take place when authorised by the Audit and Risk Manager in line with the Disposal and Decommissioning Policy

Guidance on the procedures necessary to comply with this Policy is available from the Data Controller.

This guidance covers:

- Records creation
- Business classification (for filing schemes)
- Retention periods for records
- Storage options for records
- Destruction options for records
- Archival records: selection and management
- External codes of practice and relevant legislation.

Orangebox Training discourages the retention of personal data for longer than they are required. Considerable amounts of data are collected on current staff and learners. However, once a member of staff or learner has left the organisation, it will not be necessary to retain all the information held on them. Some data will be kept for longer periods than others.

Learners

In general, electronic learner records containing information about individual learners are kept according to the requirements of the contract and individual government Commissioner and information would typically include name and address on entry and completion, programmes taken, examination results, awards obtained. Departments should regularly review the personal files of individual learners in accordance with Orangebox Training Records Retention Schedule (Appendix F). Also Archive data (Appendix I)

Staff

In general, electronic staff records containing information about individual members of staff are kept indefinitely and information would typically include name and address, positions held, leaving salary. Other information relating to individual members of staff will be kept by the Personnel Department for 6 years from the end of employment. Information relating to Income Tax, Statutory Maternity Pay etc, will be retained for the statutory time period (between 3 and 6 years).

Departments should regularly review the personal files of individual staff members in accordance with Orangebox Training Records Retention Schedule (Appendix F). Information relating to unsuccessful applicants in connection with recruitment to a post must be kept for 12 months from the interview date. Personnel may keep a record of names of individuals that have applied for, been short-listed, or interviewed, for posts. This is to aid management of the recruitment process. Individuals will be contacted and asked whether or not they would like their details to be kept on record for future vacancies. If they decline, Orangebox Training must inform them how and when their details will be permanently removed from the system.

Disposal of Records

Personal data must be disposed of in a way that protects the rights and privacy of data subjects (e.g., shredding, disposal as confidential waste, secure electronic deletion).

Publication of Orangebox Training Information

All members of Orangebox Training should note that Orangebox Training publishes a number of items that include personal data, and will continue to do so. These personal data are:

- Internal Telephone Directory.
- Information in prospectuses (including photographs), annual reports, staff newsletters, etc.
- Staff information (including photographs) on publicly accessible media (e.g. Company website).

It is recognised, that there might be occasions when a member of staff, a learner, or a lay member of Orangebox Training, requests that their personal details in some of these categories remain confidential or are restricted to internal access.

All individuals should be offered the opportunity to opt-in to the publication of any of the above (and other) data.

Where consent is not given Orangebox Training should comply with the request and ensure that appropriate action is taken.

All Orangebox Training, learners and Lay Persons have the right to opt out at any time.

Direct Marketing

Any department or section that uses personal data for direct marketing purposes must inform data subjects of this at the time of collection of the data. Individuals must be provided with the opportunity to object to the use of their data for direct marketing purposes.

Use of CCTV

Orangebox Training's use of CCTV is regulated by a separate Code of Practice.

For reasons of personal security and to protect premises and the property of staff and learners, close circuit television cameras may be in operation in certain locations. The presence of these cameras may not be obvious. This policy determines that personal data obtained during monitoring will be processed as follows:

- any monitoring will be carried out only by a limited number of specified staff
- the recordings will be accessed only by the Site Manager
- personal data obtained during monitoring will be destroyed as soon as possible after any investigation is complete
- Staff involved in monitoring will maintain confidentiality in respect of personal data.

Academic Research

Personal data collected only for the purposes of academic research (includes work of staff and learners) must be processed in compliance with the Data Protection Act 2018 (GDPR).

Researchers should note that personal data processed ONLY for research purposes receive certain exemptions (detailed below) from the Data Protection Act 2018 (GDPR) if:

- the data are not processed to support measures or decisions with respect to particular individuals, and

- if any data subjects are not caused substantial harm or distress by the processing of the data.

If the above conditions are met, the following exemptions may be applied to data processed for research purposes only:

- personal data can be processed for purposes other than that for which they were originally obtained (exemption from Principle 2)

- personal data can be held indefinitely (exemption from Principle 5)

- Personal data are exempt from data subject access rights where the data are processed for research purposes and the results are anonyms (exemption from part of Principle 6 relating to access to personal data).

Other than these three exceptions, the Data Protection Act applies in full. The obligations to obtain consent before using data, to collect only necessary and accurate data, and to hold data securely and confidentially must all still be complied with. Notes to researchers:

Whilst the Act states that research may legitimately involve processing of personal data beyond the originally stated purposes (e.g. longitudinal studies), Orangebox Training requires researchers to contact participants if it is intended to use data for purposes other than that for which they were originally collected.

Although the Act allows personal data processed only for research purposes to be kept indefinitely, researchers are asked to refer to the Ethical Advisory Committee's guidelines on Data Collection and Storage.

For those departments which gather sensitive personal data (as defined by the Act), extra care should be taken to ensure that explicit consent is gained, and that data is held securely and confidentially so as to avoid unlawful disclosure.

Researchers should ensure that the results of the research are anonyms when published and that no information is published that would allow individuals to be identified. Results of the research can be published on the web or otherwise sent outside the European Economic Area but if this includes any personal data, the specific consent of the data subject must, wherever possible, be obtained.

Physical security forms the basis for all other security efforts, including personnel and information security. A solid physical security foundation protects and preserves information, physical assets such as PC’s, laptops and office equipment as well as human assets, the employees, customers and contractors.

Security

Orangebox Training seeks to safeguard its information, physical assets and human assets by putting in place, or building into design, measures that prevent, deter, delay and detect, attempted or actual unauthorised access, acts of damage and/or violence, which trigger an appropriate response. Physical security involves the appropriate layout and design of facilities, combined with suitable security measures, to prevent unauthorised access and protection of the company’s assets, people, information, materials and infrastructure.

Physical Security

Physical security involves a number of distinct security measures which form part of a 'layered' or 'defence in depth' approach to security, which take into account the balance between risk prevention, protection and response. Physical security measures, or products such as locks and doors, are categorised according to the level of protection offered.

The 'layered' approach to physical security starts with the protection of the asset at source (e.g. creation, access and storage), then proceeds progressively outwards to include the building, estate and perimeter of the establishment. Approach routes, parking areas, adjacent buildings and utilities/services beyond the perimeter should also be considered. To ensure appropriate physical security controls, the business will consider the following factors:

- The impact of loss of the site or asset
- The level of threat and/or risk
- The perceived level of site or personal vulnerability
- The value, protective marking or amount of material held
- The particular circumstances of the establishment, including considerations of environment, location and whether occupancy is sole or shared**.**

Storage of Sensitive Assets

Critical, sensitive or protectively marked assets, like laptops, memory sticks, customer files or employee personnel records must be located in secure areas, protected by appropriate entry controls. Where there is a need to store large amounts of inherently valuable removable items, a "Secure Room" must be used.

Office Areas

A clear desk policy has been adopted. This is primarily to ensure that sensitive material such as customer files or personal staff information is not left unattended. Where it is not possible to implement a full clear desk policy, a risk assessment should take place and the decision recorded. The same principle should apply to computer screens and other office areas used to display potentially sensitive information, such as walls, notice boards etc. Computer screens should not be sited where they could be illicitly viewed (e.g. overlooked by windows or reflective surfaces).

Building Security

In any company building or location there should be as few points of exit and entry as the functions of the site and safety will allow. Where these exist, physical security controls, such as window bars, grilles, shutters, security doors etc, should be installed according to the level of risk/threat. The effectiveness of such controls may be enhanced by the use of intruder detection systems or guard services.

When choosing from the many physical security measures available, business units in conjunction with the Facilities Team should ensure that security controls are able to mitigate violent acts and deter, detect or delay intrusion – those who are not deterred should be forced to use tools and methods that facilitate detection and delay.

Physical Access Control

Access control refers to the practice of controlling and monitoring access to a property or asset. Physical access control can be achieved through a combination of manned guarding, and mechanical or technical means such as mechanical keypads or electronic door release mechanisms.

Frontline staff, such as receptionists, play a vital role in controlling access, but to be fully effective, they may need to be supported by robust customer/visitor/contractor control systems.

Frontline staff are likely to be exposed to a higher level of risk than others. This should be considered in the risk assessment and additional protections should be put in place as required including lone working arrangements and off-site visits to customers.

Incoming Mail and Deliveries

Delivered items can include letters, packets and parcels and may contain a variety of dangerous objects including blades, sharp items or offensive materials.

Anyone receiving a suspicious delivery is unlikely to know exactly which type it is, so procedures should cater for every eventuality. Refer to handling mail procedure.

Manned Guarding

If it is determined by a business unit in conjunction with the Facilities Team that onsite manned guarding is necessary the primary role of the Guard must be to provide deterrence against hostile activity and facilitate a rapid response to security incidents not to supplement Reception Staff. Guard duties and the need for, and frequency of, patrols should be decided by considering the level of threat and any other security systems or equipment that might already be in place.

CCTV

Where it is determined by a business unit in conjunction with the Facilities Team and Data Controller that CCTV is required the location must be particularly aware of the Data Protection Act Principles and the Information Commissioner's Code of Practice on CCTV, which is published under the Act. If Children or Young People under the age of 18 years are to be onsite then consent must be sought form the parents that they are happy for their child to be captured on CCTV.

Intruder Alarms

If it is determined by a business unit in conjunction with the Facilities Team that than intruder alarm is required an appropriate cost benefit analysis should be performed.

Remote/Mobile Workers

The term “remote/mobile worker” applies to employees using mobile IT devices (i.e. laptops etc) beyond the Company’s physical perimeter (i.e. premises) in the performance of their role and those authorised to work at alternative sites or from home on a permanent or regular basis. Remote/mobile working is a management option, not a universal employee fringe benefit.

All users including;

- Employees
- Contractors

- Temporary staff
- Third-party users authorised to work remotely and/or within a mobile computing environment
- Line Managers
- System Owners
- ICT system administration and technical support staff.

Authority to work remotely and/or within the mobile environment is granted by an employee's organisational line manager who must be satisfied that the employee's role can be effectively performed off-site, as required, before a remote/mobile working arrangement can commence. The line manager must be confident that the employee has the personality and work habits suitable for remote/mobile working, and that any permanent alternative work site is appropriate for the conduct of Orangebox Training business operations. Considerations for permanent/regular alternative sites should address both physical and information security aspects of Orangebox Training and partner business information, associated assets and property.

Remote/mobile workers and line managers must ensure that Orangebox Training security standards are applied to remote/mobile working environments wherever possible to ensure Orangebox Training information and information assets are not put at risk from loss or compromise. Where this cannot be achieved, alternative measures must be applied. Such alternative measures must be subject to risk assessment and management by the Orangebox Training Data Controller and approved by the Information Security Forum and/or Senior Management Team. In practice this means that employees must protect information in a similar manner no matter whether they are in an Orangebox Training office, a hotel room, or working at home.

The Orangebox Training Clear Desk and Screen Policy applies to remote/mobile workers and remote/alternate work sites. Employees must ensure that display screens for all remote/mobile systems are positioned in a manner such that they cannot be readily viewed by unauthorised persons through a window, over a shoulder, or by similar means.

Remote/mobile workers must not share passwords, tokens, smart cards or other access devices with others. Remote/mobile computing devices supplied for processing of Orangebox Training business information are provided for the exclusive use of the employee. They must not be used by, or loaned to, family members, friends or others.

Mobile devices (e.g. laptop, PDA, mobile phone, smart phone etc) should not be left unattended when not in use. Employees should pay particular attention to the safe custody of mobile devices during travel (airports, trains, hotels, baggage scans etc). Mobile computing devices (laptop, netbooks etc) are not to be left in standby/hibernate mode during travel and they are not to be left in cars or hotel rooms unless absolutely unavoidable.

Employees should also be wary of being overheard when discussing Company business over mobile phones, particularly in public places and should use guarded terms and refrain from mentioning detail beyond that needed to get the job done.

Personal Mobile phones, PDA/handheld computers etc must not be used to store Orangebox Training business information. Exceptions will be made for calendars, address books, and stored connection information such as telephone numbers.

All computers issued to Orangebox Training employees and/or associates used for remote/mobile working (desktop PCs, laptops, netbooks etc) must be protected by a Company approved drive encryption application with boot protection supplied and installed by ICT support organisation. Such products generally protect the contents of computers when the data is at rest (i.e. when

they are shut down). They do not generally protect contents after boot-up (i.e. when operating), except where files are individually encrypted. Consequently, remote/mobile computers are not to be left unattended in hibernate/standby mode and they must not be left in hibernate/standby mode during travel.

- Company Remote/mobile workers must use only Company-provided computer software, hardware, and network equipment

- All computing devices to have a fully operational personal firewall and an up-to-date anti-malware application installed or approved by ICT support organisation

- All IT users are required to check for updates on their devices on a regular (at least quarterly) basis to ensure any security patches are downloaded and installed. The Company's IT service provider also monitors devices on a daily basis for patch updates and installs them remotely as required.

- With the exception of Webmail, personally-owned computing devices are not permitted to connect to the Orangebox Training systems, or be used in any other way to process or otherwise handle Orangebox Training business information.

Employees must not change operating system configuration, disable any computer services or install new software on Company-supplied computer hardware without permission from senior management. Computer equipment supplied by Orangebox Training must not be altered or added to in any way. If such changes are required, they must be approved by senior management and be performed by ICT support organisation personnel only.

Employees must not download software from the Internet, or other external systems/sources beyond the Orangebox Training systems onto Company-provided Computers without the prior approval of senior management.

Remote/mobile workers are responsible for ensuring that their mobile systems and devices are backed up on a periodic basis, either automatically Orangebox Training systems (SharePoint, OneDrive etc) or by local independent backup devices as required. If network backup is not available or feasible, ICT support organisation will provide remote workers with the appropriate equipment. If backups are made locally, remote/mobile workers must create such backups at least weekly and store them securely in locked furniture. If these backups contain confidential information, the backups must be encrypted using an encryption solution approved and provided by ICT support organisation.

Confidential information is to be stored on-line on appropriate Company network fileservers and is not to be written to removable media without the express authority of line management. Where an acknowledged and justified business requirement exists, confidential information may be written to an encrypted USB drive/pen supplied by ICT support organisation to the individual user expressly for the purpose described. When not in use, such media is to be stored in locked office furniture and/or kept under the personal control of the individual.

Employees must receive SharePoint / OneDrive training prior to being granted privileges to access Orangebox Training systems.

Employees who have a business requirement to retain or store confidential Orangebox Training business information at their homes, or other alternative site, and have the authority of their departmental manager and the Data Controller to do so, must be provided with appropriate secure lockable furniture and approved encryption solutions for the secure storage of such information.

Remote/mobile workers authorised to work permanently or regularly from home or other alternative site are to be provided with an appropriate means to dispose of waste hard-copy confidential business information. All Orangebox Training paper-resident confidential business

information must be destroyed by CROSS-CUT shredder or other approved and contracted confidential waste disposal service. Remote/mobile workers must not dispose of confidential Orangebox Training business information in hotel wastebaskets or other publicly-accessible waste containers. Confidential business information is to be retained until it can be cross-cut shredded or destroyed by other approved methods.

When Orangebox Training supplies a remote/mobile worker with software, hardware, information or other materials (eg furniture) to conduct Orangebox Training business remotely, the title and all rights and interests to these items will remain with Orangebox Training. In such instances, remote/mobile worker possession does not convey ownership or any implication of ownership. All such items must be promptly returned to the Company when a remote/mobile worker's employment or other association with Orangebox Training ceases, or when so requested by the employees' line manager or Data Controller.

When Orangebox Training supplies a remote/mobile worker with software, hardware, information or other materials to perform Orangebox Training business remotely, Orangebox Training assumes all risks of loss or damage to these items unless such loss or damage occurs due to the remote/mobile worker's negligence or failure to comply with Company policy. Orangebox Training expressly disclaims any responsibility for loss or damage to persons or property caused by, or arising out of, the usage of such items.

Orangebox Training maintains the right to conduct physical inspections of remote/mobile worker's permanent or regular alternative sites without advance notice. Orangebox Training maintains the right to examine the contents of computers used by employees, contractors, consultants, third parties and other temporary staff, which are authorised by ICT support organisation to connect to the Orangebox Training systems and to process Orangebox Training business information, including the right to remotely inspect the contents of, and configuration of, computers used by remote/mobile workers.

Encrypted devices or encryption software must not be taken outside the UK without prior discussion and agreement with the Data Controller and senior management. This is because certain countries have specific legislation which does not permit the import of certain encryption types.

Remote/mobile workers must immediately report any loss, damage or compromise of Orangebox Training remote/mobile computer hardware, mobile phones, smart phones, software or business information entrusted to their care to the Data Controller and senior management.

Appendix A - Handling Subject Access Requests

Individuals wishing to access their personal information should submit a request in accordance with the following notes:

- Make your request, in writing, to the H.R. using the Data Protection Subject Access Request Form.
- If you have doubts about the identity of the person making the request you can ask for more information. However, it is important that you only request information that is necessary to confirm who they are. The key to this is proportionality.
- You need to let the individual know as soon as possible that you need more information from them to confirm their identity before responding to their request. The period for responding to the request begins when you receive the additional information.

- You are not required to state WHY you wish to access the information: the details we require are merely those that will aid the efficient location and retrieval of information.

- Orangebox Training adopts a general policy of openness in terms of allowing individuals access to their personal information (permitted under the Data Protection Act 2018 (GDPR).

- Once H.R. receives a Subject Access Request, all efforts will be made to fully comply within 1 month. In any event, you will receive all the information that has been located and can be released within 1 month and an explanation for any information that cannot be provided at that time.

- In accordance with the Data Protection Act 2018 (GDPR), Orangebox Training does not usually release information held about individuals without their consent. Therefore, if information held about you also contains information related to a third party, Orangebox Training will make every effort to anonymise the information. If this is not possible, and Orangebox Training has been unable to secure the relevant consent, Orangebox Training may decide not to release the information.

The Data Protection Act 2018 (GDPR) gives individuals (data subjects) a number of rights including the right to access personal data that an organisation holds about them. This right of access extends to all information held on an individual and includes personnel files, learner record files, data-bases, interview notes and emails referring to the individual. If an individual makes a request to view their information, it is known as a “Subject Access Request”. It is permissible for Orangebox Training to charge a fee of up to £10 for responding to Subject Access Requests where they are manifestly unfounded or excessive.

The Act stipulates that the data subject must:

- Make the request in writing

- Supply information to prove who they are (to eliminate risk of unauthorised disclosure)

- Supply appropriate information to help Orangebox Training to locate the information they require.

Upon receipt of a request, Orangebox Training must provide:

- Information on whether or not the personal data is processed

- A description of the data, purposes and recipients

- A copy of the data

- An explanation of any codes/jargon contained within the data.

Orangebox Training must respond to Subject Access Requests within 1 month.

Whilst data subjects are entitled to request ALL the information that an organisation holds on them, experience shows that they are usually looking for something specific.

Therefore, the majority of requests received by Orangebox Training are likely to be from staff and learners asking for copies of a specific document(s). These will usually be located from a single source - typically the departmental staff/learner files - and will not involve the disclosure of information relating to a third party. In such cases, Site policy is to be open and transparent and wherever possible to let the individual have a copy of the information with minimum fuss. Such requests should be handled directly by the relevant department or section and there should be no need to involve HR. Whilst data subjects are entitled to request ALL the information that an

organisation holds on them, experience shows that they are usually looking for something specific.

When responding to such requests, take care to ensure that you do not inadvertently release third party information without their consent. No fee should be charged.

There may be some instances when a request for information is more complex and will be handled by Orangebox Training H.R. and relevant Director to ensure a co-ordinated response. It is hoped that such requests will be infrequent.

Examples of situations where more complex requests might arise include:

- Request involves locating information from multiple sources
- Request involves the release of contentious information
- Request is one in a series of requests from the same individual
- Request involves the release of third party data for which consent has been refused or cannot be obtained
- The data subject does not want to ask for the information from the department/section that holds it.

In such cases, the request should be referred to Orangebox Training H.R. who will ensure that a coordinated approach is adopted and will determine whether or not it is appropriate to charge a fee. When responding to Subject Access Requests, the Orangebox Training H.R. will liaise with staff in the department/section as appropriate.

It will sometimes be the case that responding to a Subject Access Request will lead to incidental disclosure of details relating to some other third party (for example, a referee or another learner). Such third-party information should not be disclosed without first seeking the consent of the third party.

If consent cannot be obtained (e.g. the third party cannot be contacted) or is refused, then the institution needs to consider whether or not disclosure is reasonable, taking into account:

Any duty of confidentiality owed to the third party

- The steps taken to seek consent
- Whether the third party is capable of giving consent
- Any express refusal of consent.

If you are unable to obtain consent, you are advised to contact Orangebox Training H.R. who will have to consider/balance the impact on the third party of the disclosure, and the impact on the data subject of the disclosure being withheld. Where third parties have been acting in an official capacity it may be argued that the duty of confidence is lower than is otherwise the case. However, decisions will be made on a case by case basis.

If the H.R. decides that disclosure cannot be made, only that information which could identify the third party should be withheld (e.g. third-party details are blanked out). Wherever possible, Orangebox Training will follow good practice by explaining to the data subject that some information has been withheld, and why.

Third parties who regularly supply information on learners/staff in a professional capacity (external examiners, referees, etc) should be informed that anything they submit may become available to the data subject through a Subject Access Request.

Departments are advised to seek consent to disclose at the collection stage (e.g. when requesting references/appointing external examiners) to avoid delay upon receipt of a Subject Access Request. Where professionals request that information supplied by then be kept confidential, they must supply details of the exceptional reasons for making the request. Orangebox Training will consider those reasons in order to decide whether they are valid.

The maintenance of appropriate records is extremely important in the event of a Subject Access Request. Knowing who keeps what and where is central to the effective and efficient retrieval of information. The following guidance notes on records management have been produced to help departments and sections:

- Learner Records Management in Departments
- Learner Records Management in Support Services

The other important aspect of records management is ensuring that only appropriate information is retained. This will reduce the amount of information which must be disclosed (thereby saving time and administrative costs associated with locating and supplying the information) but will also avoid embarrassment and potential damage to Orangebox Training reputation by ensuring that inappropriate information is not being retained on individuals.

All staff are advised:

- To be careful about what personal information they keep (including emails)
- Record factual information
- Where it is necessary to record an opinion about an individual, to make sure it is justified and wherever possible backed up with factual evidence
- NOT to record anything that they would not wish the data subject to see.

There are many long-term aims of rationalising the information held by Orangebox Training. It will certainly help us to respond effectively to Subject Access Requests. The fewer data sources Orangebox Training has, the easier it will be to search these on receipt of a Subject Access Request. Wherever possible, we should be aiming to manage data on a single central database. All staff must not to hold files on individual learners or staff members, but to lodge any such information with “designated individuals” (see Records Management information referred to earlier in this section for further information). Personal data of departed staff and learners should be reclaimed from any remote sources and stored in a single location or on a single database, with appropriate security and backup.

Appendix B - Learner Records Management

The Data Protection Act 2018 gives individuals the right to access the information that an organisation holds on them. In order to comply with this part of the Act, organisations need to have in place effective means of extracting and retrieving information from a variety of sources.

Departments hold a great deal of information on their learners, usually in a variety of forms and locations. In order to comply with a subject access request, departments will need to be able to locate and collate the information quickly. It is therefore vital that key personnel (typically Head of Department and/or H.R.) know what information is held and by whom. Ideally, all information

relating to individual learners in departments should be kept in central departmental learner record files (paper or electronic) so that, in the event of a subject access request, the department can be confident that all the information is easily accessible from a limited number of central sources. However, Orangebox Training recognises that this may not always be the case in practice. Departments should ensure that departmental learner record files are as complete as possible but it is acknowledged that there may be some instances where **designated individuals*** (e.g. Disability Co-coordinators, Personal Tutors) need to retain information on learners which would not be appropriate for more general access.

Information held on learners can be categorised in one of two ways:

"Classified information" is information which a learner has requested be kept confidential between the learner and the designated individual to whom they disclose the information. Designated individuals should give learners the opportunity to define information as classified (when, for instance, unauthorised access/disclosure of the information concerned to other staff in the department poses a risk of damage/distress to the learner).

"**Unclassified information**" is all other information held on learners which will be available for general access within the department.

- Copies of unclassified information relating to an individual learner should be lodged in the departmental learner record file
- Designated individuals may retain copies of classified information without copying it to the departmental learner record file
- Designated individuals may retain duplicate copies of any documentation (whether electronic or paper), particularly if the information is consulted on a regular basis
- Members of staff, other than those responsible for the departmental learner record files and designated personnel, should not retain information (electronic or paper) about individual learners. Documentation should be filed either in the departmental learner record file or with a relevant designated individual
- Information should only be retained in accordance with the suggested retention periods in Orangebox Training Records Retention Schedule
- When a designated individual leaves Orangebox Training, they should pass all information to the member of staff responsible for learner files, to be either destroyed (in accordance with Orangebox Training records retention schedule), or filed on the departmental learner record file, or passed to a replacement designated individual
- Learners should be informed of what information is being held about them, what it will be used for, where it will be stored, and to whom it might be disclosed. This will normally be achieved via the departmental handbook, registration forms and other data collection forms.

Appendix C - Staff Records Management

The Data Protection Act 2018 (GDPR) gives individuals the right to access the information that an organisation holds on them. In order to comply with this part of the Act, organisations need to have in place effective means of extracting and retrieving information from a variety of sources.

Departments and support services sections may hold a great deal of information on their staff, usually in a variety of forms and locations. In order to comply with a subject access request, departments/sections will need to be able to locate and collate the information quickly. It is

therefore vital that key personnel (typically HR, Head of Department/Section, Line Manager and/or administrator) know what information is held and by whom.

Ideally, all information relating to individual staff should be kept in departmental staff record files (paper or electronic) so that, in the event of a subject access request, the department/section can be confident that all the information is easily accessible from a limited number of central sources. However, Orangebox Training recognises that this may not always be the case in practice. Departments/sections should ensure that staff record files are as complete as possible, but it is acknowledged that there may be some instances where **designated individuals*** need to retain information on staff which would not be appropriate for more general access.

Wherever possible, copies of documentation relating to an individual member of staff should be lodged in a departmental staff record file(s) (paper or electronic).

Designated individuals are permitted to retain duplicate copies of any documentation (electronic or paper), particularly if the information is consulted on a regular basis.

Exceptionally, designated individuals may also keep documentation relating to sensitive information (e.g. relating to health or other problems) without copying the information to the departmental staff record file. Designated individuals should only follow this practice when unauthorised access/disclosure of the information concerned to other staff in the department/section poses a risk of damage/distress to the member of staff.

Members of staff, other than those responsible for the staff record files and designated personnel, should **not** retain information (electronic or paper) about individual members of staff. Documentation should be filed either in the departmental staff record file or with a relevant designated individual.

The exception to this is email as it would be impractical for staff to pass all emails to a central source. However, all staff must be aware that in the event of a subject access request, they may be asked to search their email archives for all emails referring to the member of staff that has made the request. Therefore, staff are advised not to keep emails relating to other members of staff unless it is absolutely necessary. In writing emails referring to other members of staff, you are reminded that, in the event of a subject access request, that member of staff is entitled to receive copies of all emails which refer to them.

Information should only be retained in accordance with the suggested retention periods in Orangebox Training Records Retention Schedule.

When a designated individual leaves Orangebox Training, they should pass all information to the member of staff responsible for staff files, to be either destroyed (in accordance with Orangebox Training records retention schedule), or filed on the departmental staff record file, or passed to a replacement designated individual.

Staff should be informed of what information is being held about them, what it will be used for, to whom it might be disclosed and whether or not it will be stored in the departmental staff record file.

If these guidelines are followed, personal information held on staff can be easily located from a limited number of sources and departments will be much better prepared to respond to subject access requests efficiently

Appendix D – Disclosure of Learner Information

Orangebox Training must ensure that personal data held on learners are not disclosed to unauthorised third parties including family members, friends, and government

bodies and in certain circumstances, the Police. All staff should exercise caution when asked to disclose personal data held on learners to third parties.

Disclosing Personal Data

Personal data should only be disclosed if one of the conditions set out in Schedule 2 are met. The most likely conditions applicable to the disclosure of learner data to third parties are:

- the learner has given their consent
- the disclosure is in the legitimate interests of Orangebox Training or the third party to whom the information is being disclosed (except where this would prejudice the rights, freedoms or legitimate rights of the learner)
- statutory obligation of Orangebox Training (e.g. ESFA and other Funding Council statistical returns disclosure is required for performance of a contract.

Disclosing Sensitive Personal Data

In accordance with Principle 1 of the Data Protection Act, sensitive personal data (racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, criminal convictions) should only be disclosed if one of the conditions set out in Schedule 2 (see above) AND one of the conditions set out in Schedule 3 are met. The most likely conditions (of Schedule 3) applicable to the disclosure of sensitive learner data to third parties are:

- the learner has given their explicit (ideally written) consent
- statutory obligation of Orangebox Training (e.g. equal opportunities monitoring)
- disclosure is in the vital interests of the learner (e.g. information relating to a medical condition may be disclosed in a life or death situation).

Disclosing Personal Data Overseas

In accordance with Principle 8 of the Data Protection Act, personal data should only be disclosed outside of the EEA (the fifteen EU Member States together with Iceland, Liechtenstein and Norway) if one of the conditions set out in Schedule 4 are met.

The most likely conditions applicable to the disclosure of learner data to third parties overseas are:

- the learner has given their explicit (ideally written) consent
- disclosure is required for performance of a contract
- disclosure is necessary for the purpose of any legal proceedings.

Informing Learners of Disclosures and Obtaining Consent

Learners should be informed of predictable disclosures (such as confirmation of learner status, responding to a request for a reference) when they register with Orangebox Training. Some learners will choose to opt out of certain processing (including disclosures) on their registration form. This information is recorded on Orangebox Training database and all staff should check a learner's record before releasing any information.

In less predictable situations (e.g. taxi firm who has found wallet and wants to contact learner) where the learner has not been previously informed of a possible disclosure, the learner should give their consent before any information is released.

Orangebox Training understands "consent" to mean that the learner has signified their agreement whilst being in a fit state of mind to do so and without pressure being exerted upon them. There must be some active communication between the parties; consent cannot be inferred from non-response to a communication. In most cases, verbal consent should be acceptable so long as proper security checks are made to ensure that the person giving the consent is the learner. For telephone consent, this will mean asking the subject to confirm several separate facts that should be privy only to them (learner identity number, date of birth etc). For sensitive data, explicit written consent of learners should be obtained unless an alternative legitimate basis for processing exists (see above).

Requirement to Disclose?

Except in cases where there is a statutory obligation for an HEI to comply with a request for learner data, there is no compulsion to make a disclosure, even in cases where the Act allows this. Unless there is a legal or statutory obligation, you are advised not to disclose any personal information about learners without their consent.

Please note that disclosure includes confirmation of a learner's presence at Orangebox Training. If you are in any doubt as to the legitimacy of a disclosure, then no disclosure should be made.

Method of Disclosure

Disclosures should not be made over the telephone. The minimum-security option is to take a number and ring the enquirer back. However, it is strongly advised that all enquirers should be asked to submit their requests in writing (where appropriate on headed paper). Once you have checked whether or not the request is legitimate, you should, wherever possible, reply in writing.

Disclosure to Work Colleagues

You should always think carefully before disclosing learners' personal information to work colleagues whether they are from within, or external to, your own department. Under the Data Protection Act, you should not disclose personal data to colleagues unless they have a legitimate interest in the data concerned. As there is no definition as to what a "legitimate interest" is, it will have to be a matter of judgement in each case. As a rule, you should consider whether or not the information is necessary to allow your colleague to perform their job. So, for instance, it would be legitimate to pass information to the Exams Office regarding learner addresses, qualification classification and disabilities if special arrangements were needed to enable the learner to attend the ceremony.

When sharing information with colleagues, you should consider the level of detail necessary to enable them to perform their job. So, for instance, if you knew that a learner was going to be absent for a significant period of time, you may wish to notify colleagues in the department of this fact. However, it might not be appropriate for all colleagues to be made aware of the specific reasons (health or otherwise) resulting in the absence.

Disclosure to Relatives/Guardians and Friends

Orangebox Training has no responsibility or obligation to disclose any personal information relating to learners to relatives.

All learners are given the opportunity, both on their registration form and by email later in the year, to provide the name of a nominated individual to whom Orangebox Training may disclose personal information. You should always check a learner's record to see whether or not they have identified a nominated individual.

You may come under pressure to discuss individual learners with parents/guardians or even friends. However, in these situations it is essential that you do not disclose personal data without the prior consent of the learner - it would be a breach of the Data Protection Act to do so. If the learner has identified a nominated individual (see above) they are understood to have given prior consent.

You are, of course, free to discuss institutional procedures with parents but the specific circumstances of an individual learner cannot be discussed without the consent of that learner.

There may be occasional, exceptional circumstances (in which a learner's life or health is threatened) in which the usual need to get consent before disclosing to parents/guardians may be waived. Orangebox Training holds details of learner's '"next of kin" or for such purposes.

Confirmation of Learner Status and Award

Learner status is regarded as personal data and therefore must be processed in accordance with the Data Protection Act; this includes protecting the information against unauthorised disclosure. By confirming whether or not an individual is (or has been) registered at Orangebox Training could be a breach of the Act.

Orangebox Training receives enquiries regarding individuals' learner status on a regular basis. The nature of the third party requiring the information can range from current or prospective employers genuinely trying to confirm details on a job application form to estranged or abusive partners trying to trace an individual's whereabouts. Therefore, whenever faced with a request for confirmation of learner status, you should exercise caution before responding. You should always employ appropriate security measures to check the identity of the enquirer and you should not disclose the information over the telephone. Wherever possible, ask the enquirer to put their request in writing, preferably on headed paper.

For other enquirers, where there is no statutory or other legal obligation for you to disclose information, you should not confirm or deny the learner status of an individual without their consent.

Disclosure to current and prospective Employers and Educational Institutions

You may receive requests for information regarding individual learners (current or former) from current/prospective employers/educational institutions. Typically, this occurs when the learner has applied for a job or a place on a programme of study. The disclosure will usually be in the best interests of the learner and more often than not, the learner will be aware that such a request would be made. The information released should be kept to a minimum - usually registration status and/or award. As always, care must be exercised in the method of disclosure. See Section 8 for more detail on Personal References.

Requests for Personal References

If you receive a request for a personal reference relating to a learner, you should ensure that:

- the information contained in the reference is FACTUALLY correct
- where possible, keep the disclosure to a minimum (learner's dates of study, registration status)

- sensitive data (e.g. details of health to explain absences from Orangebox Training) must **not** be disclosed without the explicit consent of the learner where opinions about a person's suitability are disclosed, your comments are defensible and justifiable on reasonable grounds

- if you are unable or unwilling to give a reference, such a refusal is communicated carefully, without, in effect, implying a negative reference and thus disclosing personal data

- you do **not** disclose any information if asked to give an unsolicited reference (for a learner who has not, to your knowledge, cited your name as a referee).

The identity of the person requesting the reference should always be confirmed prior to disclosure. Requests for references should usually be made in writing on headed paper. If you receive an email request for a reference, you should be assured that it is a valid request. If it is from a known source or company domain, you should process the request, but you may wish to reply in written format to a known postal address for the company/organisation. If the email domain is not familiar, you are advised to investigate further.

Telephone references are not usually recommended. However, they are acceptable if the learner has specifically asked you to provide a reference at short notice. As a minimum-security measure, it is recommended to ring the enquirer back to check that they are who they claim to be.

If a learner cites your name as a referee, it is understood that they are giving consent for you to disclose information (regardless of whether they have opted out on their registration form). **If you are not aware that a learner has cited you as a referee, you should check the validity of the request.**

Disclosures to the Police and Legal Proceedings

Disclosures to the Police are NOT compulsory except in cases where Orangebox Training is served with a court Order requiring information. However, Section 29 of the Data Protection Act 2018 does allow limited exemptions from the first Principle meaning that Orangebox Training may release information to the Police without the consent of learners in limited circumstances.

Such disclosures should only be made if the Police confirm that they wish to contact a named individual about a specific criminal investigation and where Orangebox Training or believes that failure to release the information would prejudice the investigation. Staff must not release information to the Police over the telephone. The Police must inform Orangebox Training in writing. Most Police Forces will have their own request form which should always include a statement confirming that the information requested is required for the purposes covered in Section 29, a brief outline of the nature of the investigation, the learner's role in that investigation, and the signature of the investigating officer.

Legal Proceedings the Act exempts data from the nondisclosure provisions (e.g. obtaining consent from learner) in cases where disclosure is necessary "for the purpose of, or in connection with, legal proceedings…..or for the purpose of obtaining legal advice, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights". In practice this means that Orangebox Training can disclose information regarding learners to its own solicitors when seeking proper legal advice about a case. However, for cases that do not directly involve Orangebox Training, information should only be disclosed if the relevant learner's permission can be obtained. If the information is vital to a case, a Court Order may be issued demanding the information. There are sections that specifically allows data controllers to disclose without consent from the data subject (learner) when confronted with a Court Order.

Audit

Orangebox Training will appoint external and internal auditors who will see some learners' personal data during the course of their investigations. Audits of the learner record are also conducted by our contracts. Learners are made aware of this possibility when they register and therefore, in registering, give their consent for disclosure to auditors.

Survey/Research Organisations

Survey/Research Organisations may approach you for a list of addresses or emails for learners in your department so that they can market their services or circulate a survey. You must not release this information but instead can offer to mail the information/survey on their behalf. If you do decide to undertake a host mailing, you should include a statement explaining the context of the mailing and reassuring learners that their personal data have not been released to the third party.

Forwarding Learner Correspondence on behalf of a Third Party

You should not release learner addresses or contact details to a third party without the consent of the learner. Instead, you may offer to forward correspondence to a learner on behalf of a third party. Sometimes you may even receive unsolicited correspondence with a request to forward it to a learner. You must take care when handling such requests. Remember that an individual's learner status is personal data. Therefore, if you receive such a request, it is important to neither confirm nor deny that that person is a learner at Orangebox Training.

Appendix E - Telephone Protocol for the Disclosure of Personal Information

Orangebox Training must ensure that personal data held on individuals are not disclosed to unauthorised third parties including family members, friends and government bodies and in certain circumstances, the Police. All staff should exercise caution when asked to disclose personal data to third parties. These guidance notes are intended to provide guidance for staff that deals regularly with telephone calls from third parties requesting personal data on learners and staff and should be read in conjunction with Orangebox Training Data Protection Policy.

Disclosing Personal Data

In accordance with Principle 1 of the Data Protection Act, personal data should only be disclosed if one of the conditions set out in Schedule 2 are met. The most likely conditions applicable to the disclosure (over the telephone) of learner or staff data to third parties are:

- The learner or member of staff has given their consent
- The disclosure is in the legitimate interests of Orangebox Training or the third party to whom the information is being disclosed (except where this would prejudice the rights, freedoms or legitimate rights of the learner or member of staff)
- Disclosure is required for performance of a contract (e.g. contract between a learner and their sponsor).

Disclosing Sensitive Personal Data

In accordance with Principle 1 of the Data Protection Act, sensitive personal data (racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, criminal convictions) should only be disclosed if one of the conditions set out in Schedule 2 (see above) AND one of the conditions set out in Schedule 3 are met. The most likely conditions (of Schedule 3) applicable to the disclosure (over the telephone) of sensitive learner or staff data to third parties are:

- The learner or member of staff has given their explicit (ideally written) consent
- Disclosure is in the vital interests of the learner or member of staff (e.g. information relating to a medical condition may be disclosed in a life or death situation).

Disclosing Personal Data Overseas

In accordance with Principle 8 of the Data Protection Act, personal data should only be disclosed outside of the EEA (the fifteen EU Member States together with Iceland, Liechtenstein and Norway) if one of the conditions set out in Schedule 4 are met. The most likely conditions applicable to the disclosure (over the telephone) of learner or staff data to third parties overseas are:

- The learner or member of staff has given their explicit (ideally written) consent
- Disclosure is required for performance of a contract
- Disclosure is necessary for the purpose of any legal proceedings

Consent

Orangebox Training understands "consent" to mean that the learner or member of staff has signified their agreement whilst being in a fit state of mind to do so and without pressure being exerted upon them. There must be some active communication between the parties; consent cannot be inferred from nonresponse to a communication. In most cases, verbal consent should be acceptable so long as proper security checks are made to ensure that the person giving the consent is the learner or member of staff. For telephone consent, this will mean asking the subject to confirm several separate facts that should be privy only to them (learner/staff identity number, telephone number, date of birth etc). For sensitive data, consent should NOT be obtained over the telephone and explicit written consent of learners or staff should be obtained unless an alternative legitimate basis for processing exists (see above).

Internal (within ORANGEBOX TRAINING) Disclosures by Telephone

You should always think carefully before disclosing learner or staff personal information to work colleagues whether they are from within, or external to, your own department. Under the Data Protection Act, you should not disclose personal data to colleagues unless they have a legitimate interest in the data concerned. As there is no definition as to what a "legitimate interest" is, it will have to be a matter of judgement in each case. As a rule, you should consider whether or not the information is necessary to allow your colleague to perform their job. When sharing information with colleagues, you should consider the level of detail necessary to enable them to perform their job.

If you can identify the member of staff making the telephone enquiry (e.g. from their voice) and you are satisfied that they have a legitimate reason for requesting the personal information, you may disclose this over the telephone. Take care to ensure that in disclosing the information over the phone, you are not inadvertently disclosing the information to other members of staff. This is

particularly important in the case of sensitive personal data and for staff working in an open plan office.

If you cannot be sure of the identity of the member of staff making the telephone enquiry, you should ask them to put the request in writing (email is preferable) so that you can deal with it at a later stage. Again, before releasing the information, you need to be satisfied that the member of staff is requesting the data for a legitimate purpose. Ask the enquirer to indicate what they will be using the information for and keep the written communication as background evidence should the disclosure be questioned at a later date. To avoid embarrassment, you could say that you do not have the information to hand and that you need time to find it and get back to them. Alternatively, you could offer to take a contact telephone number and call them back later once you have gathered the information.

External (outside Orangebox Training) Disclosures by Telephone

In general, disclosures to external bodies/companies/agencies/individuals should not be made over the telephone. It is strongly advised that you ask enquirers to submit their requests in writing (where appropriate on headed paper). This will give you time to check whether or not the request is legitimate and where possible obtain consent for the disclosure from the member of staff or learner about whom information is requested. You should, wherever possible, reply to the request in writing.

Orangebox Training recognises that in some, exceptional situations, time constraints and other factors make it a necessity to disclose information over the telephone. If you find yourself in a position where it is necessary to disclose information over the telephone, you should take a contact number and ring the enquirer back. This will go some way to ensuring that the caller is who they say they are. Even the above procedures could be subject to fraud and should only be used when no other alternative exists. In such cases Orangebox Training should at least be regarded as having taken reasonable precaution given the circumstances - i.e. that the security in place was appropriate to the risk involved in unlawful processing of data. As always, particular care should be taken when disclosing sensitive personal data or information that could potentially cause the learner or member of staff to suffer subsequent damage and/or distress.

Please note that even confirming whether or not a learner or member of staff studies or works at Orangebox Training could be a potential breach of the Act.

Disclosure to Parents (Learner Information)

Orangebox Training has no responsibility or obligation to disclose any personal information relating to learners to parents or other relatives.

You may come under pressure to discuss individual learners with parents/guardians or even friends over the telephone. However, in these situations it is essential that you do not disclose personal data without the prior consent of the learner - it would be a breach of the Data Protection Act to do so.

You are, of course, free to discuss Orangebox Training procedures with parents but the specific circumstances of an individual learner cannot be discussed without the consent of that learner.

There may be occasional, exceptional circumstances (in which a learner's life or health is threatened) in which the usual need to get consent before disclosing to parents/guardians may be waived. Orangebox Training holds details of learners' "next of kin" for such purposes.

What to do if someone calls claiming to be a learner

You may receive telephone calls from individuals claiming to be learners. Unless you are 100% sure that the person on the line is who they claim to be, you should not disclose information over the telephone. You are advised to ask for confirmation of the learner's username, home address and date of birth before proceeding with the call. If the caller can provide the details accurately, make a note of the information that they require and inform them that you will send it to their email address. If this is not possible and the caller insists that they need the information urgently, you may take a contact telephone number and call them back with the information.

Home Addresses, Telephone Numbers and E-mail addresses

You should never give out **personal/home** addresses or telephone numbers of staff or learners to third parties over the telephone unless you have been given explicit (in writing) permission by the individual. Instead you could **t**ake the caller's contact details and say you will pass a message asking the learner or member of staff to contact them offer to forward correspondence to a learner or a member of staff on behalf of the caller. You must take care when handling such requests. Remember that an individual's learner/staff status is personal data. Therefore, if you receive such a request it is important to neither confirm nor deny that that person is a learner or member of staff at Orangebox Training.

However, it would usually be deemed appropriate to disclose a colleague's **work** contact (telephone and departmental address) details in response to an enquiry regarding a particular function for which they are responsible. If you are asked to disclose another member of staff's email address, you should ask the caller to send the email to you and inform them that you will forward the message on to the individual they are trying to contact if they are a member of Orangebox Training. It would not usually be appropriate to disclose a colleague's work details to someone who wished to contact them regarding a nonwork-related matter.

References

Telephone references are not usually recommended. However, they are acceptable if you have been specifically asked by a learner or a member of staff to provide a reference at short notice. The identity of the person requesting the reference should always be confirmed prior to disclosure. As a minimumsecurity measure, it is recommended that you ring the enquirer back to check that they are who they claim to be.

When disclosing information in the form of a personal references please ensure that:

- The information you disclose is FACTUALLY correct
- The disclosure is kept to a minimum
- Sensitive data are **not** disclosed without the explicit consent of the learner or member of staff
- Where opinions about a person's suitability are disclosed, your comments are defensible and justifiable on reasonable grounds
- If you are unable or unwilling to give a reference, such a refusal is communicated carefully, without, in effect, implying a negative reference.

Disclosures to the Police

Disclosures to the Police are NOT compulsory except in cases where Orangebox Training is served with a court Order requiring information. However, The Data Protection Act 2018 (GDPR) does allow Orangebox Training to release information to the Police WITHOUT the consent of

learners or members of staff in LIMITED circumstances. Such disclosures should only be made if the Police confirm that they wish to contact a named individual about a specific criminal investigation and where Orangebox Training believes that failure to release the information would prejudice the investigation. If you are contacted by the Police and are not sure how to deal with their request, you can get in touch with the Data Protection Officer or staff in the Security Office for advice on how to deal with the enquiry.

The Police MUST request the information from Orangebox Training in writing. You are NOT obliged to release information to the Police over the telephone. Most Police Forces will have their own request form, which should always include:

- A statement confirming that the information requested is required for the purposes covered
- A brief outline of the nature of the investigation
- The data subject's role in that investigation
- The signature of the investigating officer.

Conclusion

The purpose of the Data Protection Act 2018 (GDPR) is to protect the rights and privacy of individuals with regard to their personal information. At times you may feel like you are being obstructive to callers asking for information about learners or members of staff. In these cases, explain that the information falls under the Data Protection Act 2018 (GDPR). Follow the above guidelines in a courteous and professional manner and in most circumstances, you should not experience too many problems. However, if you are faced with a particularly difficult caller, do your best to diffuse the situation without losing your temper. Explain that you are following guidelines approved by Orangebox Training and that by providing the information over the telephone; you could be breaking the law. Orangebox Training has adopted some standard phrases to help you. Remember:

- There is no such thing as a Data Protection emergency (except where someone's life or health may be at risk). You are well within your rights to stall a caller whilst you seek further information and advice
- If in doubt contact Orangebox Training Data Controller.

Appendix F Records Retention Schedule

Orangebox Training – Records Retention Schedule (records containing personal information)

The following minimum retention periods relate to all personal information, regardless of the format in which it is stored. The list is not exhaustive but provides guidance as to best practice.

- Health and Safety Records: **6 Years**
- Employee Records: **3 Years**
- Learner Records: **6 Years**
- External Examiner and Invigilator Records: **6 Years**
- Financial records as required by HMRC.

Appendix G Examinations and Assessment

- Subject Access Requests Exam scripts, Examiners Comments [including external examiners comments] Pre-Programme Board/ Programme Board and Module Board Reports Automated decision making

- Publication and Release of Results

- Additional Needs Learners.

Subject Access Request

Under the Data Protection Act 2018 (GDPR), learners have the right to request to see a copy of all information held on them by Orangebox Training. This right extends to various documents/information collated during the examinations and assessment process.

Publication and Release of Results

- Examination results (includes other forms of assessment) are personal data and therefore should not be disclosed to third parties without consent. This includes the common practice of publishing results via posting on public noticeboards, as well as the announcement or publication of results

- Under the Data Protection Act 2018 (GDPR), Orangebox Training has an obligation to explain to learners where their results may be published and to provide a mechanism

- through which they can object to their results being displayed in all or any particular form (includes email notification). The Registry will undertake to email learners to explain where, and how, learners might expect to see their results published

- If a learner asks to see a copy of their results, Orangebox Training must provide access to all examination marks either within 5 months of the request or 1 month after the official release of results (whichever is sooner). Learners can request a hard copy of information held, in which case a written statement or printout of results will have to be provided

- As there is no sure way of confirming the identity of a caller, the risk of unauthorised disclosure of examination results over the telephone is high.

Therefore, examination results should never be released over the telephone. All learners receive confirmation of their results within 48 hours by post and some departments have adopted the practice of emailing learners' results to them. Whatever method of disclosure is chosen, it is important to manage learner expectations carefully.

Appendix H Photographs to be used in Publicity / Promotional Material

These guidance notes cover the provision and receipt of references for both staff and learners and should be read in conjunction with Orangebox Training Data Protection Policy

General Photographs

If individuals are not readily identifiable from the photograph and it seems unlikely that any damage or distress will result from such processing, then it will not be necessary to obtain consent. Therefore, learners and staff whose images appear as incidental detail in publicity photographs will not need to give consent for the use of their image.

Photographs of Group Activities

Where photographs are to be taken of a group activity then this should be announced in advance so that individuals may leave the room briefly if they do not wish to appear in the photographs.

Photographs of Small Groups/Individuals

Where photographs are to be taken of a single individual, or a small group of individuals, where individuals are the main subject of the photograph (even if they are not identified by name), consent should be sought before any photographs are taken. When gaining consent, it is important to ensure that individuals are informed of what the images will be used for (e.g. where they will be printed and who will have access to them).

Publishing Photographs on the Web

images appear as incidental detail) are to be published on the Internet If it is intended to make photographs available on the web, wherever possible this should be restricted to the Intranet rather than the Internet. Publishing on the Internet potentially transfers personal data outside of the EEA (the fifteen EU Member States together with Iceland, Liechtenstein and Norway) for

which rules on gaining consent from individuals are much stricter. If photographs (except where learner/staff, written consent should be obtained from the subject(s).

Appendix I – Archiving Data

Orangebox Training shall maintain original invoices; management information returns and all other documents necessary to verify the Service provided in relation to its contracts for 6 years following the expiry or termination of the agreements unless otherwise required specific to each contract.

We shall also maintain Customer, Learner and staff records for 6 years following the expiry or termination of their employment, course or agreements.

Once the data to be archived is identified, it is the responsibility of the department to undertake the following actions:

- Ensure that all documents are within the file, disc or folder
- Label the file, disc or folder with name, contract, date and contents. e.g. (learner base folder) –
  (employee HR folder) – (Contractor agreements, schedules)
- Use the Archive Data sheet to record the data that is being archived. (See below)
- Enclose data files in archive box with all the data files, folders or disc and give to the data controller for Orangebox Training
- Data Controller to add date, box number, contents, etc to the Archive Spread Sheet and check content of archived information
- Seal archive box ensuring everything list is contained in box with the archive data sheet enclosed
- File original signed Archive Data sheet in manual leaver arch file
- Contact External Archive Company (Restore) for collection
- File Receipt from Archive Company with each archive data sheet.

Retrieving Data

If there is a reason for retrieving data, you will need to follow the step below: Contact the Data Controller and explain what needs to be retrieved and why. This should be made in writing/ email.

- The data controller will need to ensure that the person requesting the data has the necessary authority
- Once the Data Controller is happy with the request and the box needs to be identified from the
  Archived data spread sheet. A request to the external company needs to be made

- There is a cost associated to this process, so Orangebox Training purchase order request needs to be undertaken

- On receipt of the archived data, any documentation removed needs to be recorded, signed for with the data controller and then replaced.

For further guidance or advice on the Data Protection Act 2018 (GDPR), please contact the Data Controller.

Data Breaches

All data breaches will be reported to the Data Controller, and the Data Controller will record and investigate and where necessary inform external bodies such as Funding Commissioners/bodies and the ICO of the breach.

Processes and procedures will be revisited and retraining for those involved or instigation of relevant H.R.
processes e.g. disciplinary/dismissal procedures.

The SMT will utilise reports to identify and implement further actions to diminish future potential breaches.

The Data Controller will update the Risk Register.

Appendix J – Data Archive Sheet Handling Subject Access Requests

Data Archive Sheet

Box Number: _____

Added to Archive Spreadsheet by: _____

Date Sent to Archive: _____

Name of Item/ Learner/ Employer/ Employee/ SubContractor	Contract/ Department	Contents Archived	Date Archived	Signed in By

Appendix K – Data and Information Security

Data and Information Security

Document Abstract

This document is here to outline the implementation of information technologies to assist as measures to the compliance with the General Data Protection Regulations (GDPR).

Protection of Confidential Data

All IT Systems are protected by centralised authentication and rights of access. This system provides a central user database for the internal IT Resources and Office365 as well as other 3rd party resources which can leverage Office365 as an authentication mechanism. Managed Computers are protected via Bitdefender Endpoint Protection with live monitoring by the IT Support Team.

Most Endpoints such as Desktops, Laptops and Remote Desktop systems have disk encryption enabled, except for those devices not under direct management of IT or are using the Windows Home Edition of the Microsoft Operating System. For noncompliant Operating Systems or Computers not under the direct supervision of IT Support, SharePoint has been configured to prevent the downloading of information to such devices.

External access from devices not managed by IT Support or located outside of the Orangebox Training Solutions premises have multi-factor authentication enforced as additional measures to conventional password encryption.

Password policies have been enforced to ensure passwords are changed every 120 days, historical passwords are not reused, and the password meets minimum password complexity. Employees credentials have a threshold where their account will be locked out after multiple failed authentication attempts.

Restriction on Access to Confidential Data

Orangebox Training Solutions have shared storage spaces relevant to the individual teams and departments where respective information can be shared amongst them. Employees such as Directors and Management, except for Safeguarding, have access to all shared storage spaces and departments and can add and remove employees from teams and departments.

Safeguarding Data

Information relating to Safeguarding is strictly controlled and audited. Audit information on file access is available to all Employees of the Safeguarding team. IT Support have access to audit, backup and manage data within this team but under the strict instruction of not to view the data itself unless under the written instruction of the Safeguarding Team Lead.

Accountability and Auditability

Internal IT resources and Office365 including Exchange, SharePoint, OneDrive and Teams have been configured to record a full, unearnable historical record on information being accessed, shared, created and edited.

All systems have been configured to default to storing data on OneDrive and SharePoint to adhere to compliance. Audit information is accessible in the Office365 Security and Compliance Centre.

Data stored within the Office365 platform can be searched for and audited by keywords.

Secure Access and Revoke of Access

OneDrive and SharePoint allow entire folders and individual files to be shared with external parties to the organisation securely whilst the data is retained on a storage medium under the provision of Orangebox Training Solutions.

Essentially sharing a link with such parties to access the data, this link can be administratively revoked at any time by Data Protection Officers, IT Support and employee who initiated the sharing of data.
This then also leads to additional auditing, access and sharing of data via the 3rd party.

Microsoft Security and Compliance Centre

This resource made accessible to the appointed Data Protection Officer, and IT Support; allows full visibility into the management, security, and processing information within the Office365 platform.

You can learn more about this resource via the following resource:

https://go.microsoft.com/fwlink/p/?LinkID=2111376&clcid=0x809&culture=en-gb&country=GB