Xact Consultancy and Training Limited

Data Management Policy

1. Policy principles

1.1 Introduction

This policy explains how Xact Consultancy & Training Limited (Xact) manages personal data of employees, students, contractors (Data Processors), customers and suppliers.

It demonstrates how Xact complies with the General Data Protection Regulation (GDPR) which is regulated by the Information Commissioner's Office (ICO).

The GDPR superseded the Data Protection Act (DPA) on 25th May 2018.

1.2 Key definitions

This policy contains a number of key definitions which are set out in Section 8.1 of this policy.

1.3 Scope of policy

This policy applies to all Xact employees, Data Processors, students and others who use or process personal data. This policy applies regardless of where personal data is held and or the equipment used if the processing is for the Xact's purposes. Further, the policy applies to all personal data, sensitive personal data or special category data held in any form whether manual paper records or electronic records.

1.4 General principles

Xact complies with the principles of good information handling, including:

a) Processing personal data fairly and lawfully.
b) Processing only as much information as we need to carry out Xact's activities. This will include course booking, eligibility for attending courses, payment details, accommodation requirements, course assessment and feedback, qualification registration.
c) Taking reasonable steps to ensure personal data is accurate and up to date.
d) Keeping personal data only for as long as is necessary.
e) Keeping personal data securely and not passing it to anyone outside the company without just cause.
f) Not transferring personal data without adequate protection.

1.5 Information Commissioner

Xact is registered with the Information Commissioner for the types of information it holds and the purposes for which it process personal data.

The company's registration number is: Z9001396

1.6 Communication

This policy will be communicated to all employees and Data Processors on induction, changes to policy and on other appropriate occasions.

1.7 Website Privacy Policy

See also Website Privacy Policy.

1.8 Review

This policy will be periodically reviewed.

2. Roles and responsibilities

2.1 Directors

Xact's board of directors are responsible implementing this policy

2.2 Data Protection Officer

Xact's Data Protection Officer (DPO) is responsible for:

a) compliance with the DPA and GDPR
b) compliance with this policy
c) detecting, investigating and reporting a breach of personal data
d) primary point of contact for DPA and GDPR
e) reviewing this policy

2.3 Data Controller

Responsible for the way in which personal data is stored, used and processed.

2.4 Data Manager

The Data Manager is responsible for the day to day management of personal data and compliance with this policy.

2.5 Employees and Data Processors

All employees and Data Processors must comply with this Policy whenever processing personal data held by Xact or on behalf of Xact.

2.6 Students and co-ordinators

All students are responsible for compliance with this policy where collecting and processing personal data as part of their educational process e.g. course, studies etc.

3. Information we hold

3.1 Principles underpinning the information we hold

Xact will only store personal information necessary to enable it to conduct its business. We will only hold Sensitive Personal Data when there is a clear requirement e.g. employee's health details and information necessary to make reasonable adjustments[1].

[1] See policies at end of section 3.3

3.2 Employees and Data Processors

The personal information we hold for employment and service delivery purposes may include:

a) Full name and title
b) Gender
c) Home address
d) Personal email address
e) Personal telephone number/s
f) Emergency contact details
g) Doctors contact details and health information
h) Employment details e.g. National insurance number, pension arrangements, bank details, tax coding, annual leave, sickness etc.
i) Identity information e.g. Photo ID: e.g. driving licence or passport

3.3 Students

The personal information we hold for educational and awarding body registration purposes may include:

a) Full name and title
b) Gender
c) Dietary information
d) Employers and co-ordinators contact details
e) Accommodation requirements
f) Interest in Xact's services
g) Payment history and details
h) Contact details e.g. email address and telephone numbers
i) Information relevant to submission deadline extensions[2], reasonable adjustments[2] and qualification registration[2]

j) Identity information[2] e.g. UK address, photo ID: e.g. driving licence or passport

k) Information to determine eligibility for attending courses

[2] See policies:

52 Registration and Certification

53 Submission Policy

62 Identity Confirmation Policy

63 Reasonable Adjustment Policy

3.4 Suppliers

The personal information we hold for business purposes may include:

a) Full name and title

b) Contact details e.g. email address and telephone numbers

4. Processing personal data

4.1 Principles of processing personal information

The processing of personal information will only be carried out where one of the following conditions has been met:

a) The individual (Data Subject) has given their consent
b) It is necessary for the performance of a contract with the individual
c) A legal obligation exists
d) It is in the individual's interest
e) It is necessary for the administration of justice
f) The benefits are for the legitimate interests of the company and do not outweigh any detriment to the individual

4.2 Confidentiality

a) Any information provided to Xact will remain confidential and only be used for the purposes for which it has been disclosed.
b) Unless Xact has permission, we will not sell, distribute or lease personal and confidential information to third parties, unless we are required by law to do so.

4.3 Data Subjects rights

With regards to the personal information we store, data subjects have rights to:

a) **Receive a copy** of the personal information we hold about them and that we are lawfully processing their data
b) **Request correction** of the personal information that we hold about them.
c) **Request erasure** of their personal information. This enables them to ask us to delete or remove personal information where there is no justification for us continuing to process it.
d) **Object to processing** of their personal information where we are relying on a legitimate interest (or those of a third party) and there is something about their particular situation which makes them want to object to processing on this ground. They also have the right to object where we are processing their personal information for direct marketing purposes.
e) **Object to automated decision-making including profiling**, that is not to be subject of any automated decision-making by us using their personal information or profiling of them.

f) **Request restriction of processing** of their personal information. This enables them to ask us to suspend the processing of personal information about them, for example if they want us to establish its accuracy or the reason for processing it.

g) **Request transfer** of their personal information in an electronic and structured form to them or to another party (commonly known as a right to "data portability"). This enables them to take their data from us in an electronically useable format and to be able to transfer their data to another party in an electronically useable format.

h) **Withdraw consent.** In the limited circumstances where they may have provided their consent to the collection, processing and transfer of their personal information for a specific purpose, they have the right to withdraw their consent for that specific processing at any time. Once we have received notification that they have withdrawn their consent, we will no longer process their information for the purpose or purposes they originally agreed to, unless we have another legitimate basis for doing so in law.

4.4 Consent for processing activities

We normally only process personal data for the following activities:

a) Record keeping e.g. courses attended, dietary requirements, reasonable adjustments etc.

b) Qualification registration

c) Notification of course/RPL assessments, re-submission requirements etc.

d) Posting of certificates and evidence submissions

e) Expression of interest in the services Xact provide

f) Marketing for activities in which organisations and individuals have shown an interest

g) Taking credit and debit card payments.

4.5 Data subject access requests

Individuals can submit a written email request to datacontroller@xact.org.uk regarding what personal information is held about them, how it is processed and the circumstances in which it is disclosed.

This will normally be completed free of charge and within one month of the request.

Should the request be manifestly unfounded, excessive or repetitive then we may refuse or charge for responding.

If we refuse a request, we will inform you why your request has been refused. If this occurs you have a right to complain to the supervisory authority and to a judicial remedy.

5. Data Protection

5.1 Principles of data protection

To prevent unauthorised access or disclosure of personal information, we have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information we collect.

5.2 Responsibilities

The Data Protection Officer is responsible for the security of electronic and hard copies of personal data.

5.3 Employee and Data Processor responsibilities

Employees and Data Processors are responsible to:

a) manage personal information to which they have access e.g. each employee and Data Processor is responsible for the information they access, receive, store, use, disclose and process.
b) ensure that personal information is kept secure at all times and is not disclosed to unauthorised persons.
c) ensure that any locked stores remain locked and keys kept secure.
d) keep IT password/s secure. See password policy detailed in IT Systems Policy

5.4 Access to information

a) Access to information will be restricted to authorised personnel only.
b) Each authorised person will be restricted to accessing information relevant to the areas necessary to carry out their role.
c) The Administration Manager is responsible for identifying the level of access for each employee.

5.5 Hard/paper based records

a) Paper records with personal information are kept in a locked store.
b) Access is only available to authorised personnel.
c) Personal information will only be disclosed to those who require access to carry out their roles and for the purposes for which it was provided e.g. assessment, qualification registration, investigation etc.
d) When the information is no longer required, it will either be returned to the person concerned, shredded or archived in a locked store.

5.6 Electronic information

a) Electronic information is stored in a secure area on Xact's server.

b) Access is password protected.

c) Access is only available to authorised personnel.

5.7 Disposal of personnel information

Personal information no longer required will be disposed in following manner:

a) Personnel information stored on paper will be shredded before disposal.

b) Personnel information stored electronically will be wiped.

Note: See Environmental Policy on disposal of electronic equipment

6. IT Security

6.1 Principles of IT Security

Xact's IT systems has been designed to achieve the following objectives:

a) Comply with business IT best practice
b) Store information in an efficient manner
c) Prevent unauthorised access
d) Provide contingency in disruption due to fire, theft, mains failure, hardware or software failure or loss of internet connection

6.2 IT equipment

This applies to Xact's IT systems and includes the following equipment:

a) Server and database
b) Data-storage and back-up systems
c) Desktop computers at main office
d) Desktop computers at remote offices
e) Employee laptops
f) Contractor laptops
g) Delegate laptops
h) Course material on a secure area of Xact's website

Note: For more information about contingency arrangements see: Business Continuity Policy.

6.3 Access

Access to IT system is at the following levels:

a) **Administrator level**: Those who have access to all areas of Xact's systems. The Managing Director and Xact's IT Support Contractor have access at this level.
b) **Employee level**: Those who have access to designated areas of the server, databases, website, desk top computers and laptops.
c) **Contractor level**: Those who have access to designated course, assessment and internal verification material on Xact's database.
d) **Delegate level:** Those who have access to designated areas of laptops and secure information on Xact's website.

6.4 IT System management

Xact have a maintenance contract with M Technical Limited to manage Xact's IT systems. M Technical are a Microsoft Partner and ensure we comply with the highest industry standards.

6.5 Security protection

Security protection for the IT Systems is ensured as follows:

a) Server has firewall, antivirus and mail server security protection
b) Access to server files is restricted to administrators
c) All computers have up-to-date firewall and antivirus protection
d) The servers, databases, back-up systems and computers are password protected and require personal login
e) All personnel are provided with personal login username and password
f) Delegate laptops cannot connect into the server or back-up systems.
g) Access to internet sites relevant to workplace role is restricted

6.6 Third party accreditation

Xact IT Systems are third party accreditation in its compliance with the Cyber Essentials scheme.

Cyber Essentials is a government-backed, industry supported scheme to help organisations protect themselves against common cyber-attacks.

6.7 PCI DSS Compliance

Xact accepts credit card payments and complies with the Payment Card Industry Data Security Standard (PCI DSS).

Xact's IT systems have been assessed and is maintained as being PCI DSS Compliant.

7. Personal Data Breaches

7.1 Personal Data Breach

Any employee, Data Processor, student or supplier who knows or suspect an actual or potential personal data breach has occurred must immediately notify the Data Protection Officer by email: datacontroller@xact.org.uk

All individuals are responsible for fully engaging and cooperating with the Data Protection Officer in relation to an investigation of a personal data breach.

7.2 Response

Xact will respond promptly to any identified personal data breaches and thoroughly investigate those incidents to ascertain whether:

a) The breach should or must be reported to the ICO
b) Data subjects should or must be made aware of the breach; *and*
c) It is necessary to amend processes or introduce new measures to mitigate against any further breaches.

8. Definitions and roles

8.1 Key definitions

Data Controller: Person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed

Data Processor: An organisation or contractor which processes personal data on behalf of a Data Controller.

Data subject: Living individual to whom personal data relates

DPA: The Data Protection Act 1998 which was superseded by the GDPR on 25th May 2018

GDPR: General Data Protection Regulation which superseded the DPA on 25th May 2018

ICO: Information Commissioner's Office, the Regulator

Personal Data: Any information relating to an identified or identifiable individual; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number.

Personal Data Breach: A confirmed incident in which sensitive, confidential or otherwise protected data has been accessed and/or disclosed in an unauthorised fashion

Sensitive Personal Data: Information concerning a data subject's racial or ethnic origin, political opinions, religious beliefs, trade union activities, physical or mental health, sexual life, or details of criminal offences.

Students: Delegates, applicants, those receiving training and qualifications

Xact: Xact Consultancy & Training Limited

8.2 Roles

Data Controller:	Managing Director
Data Manager:	Administration Manager
Data Protection Officer:	Managing Director
IT Support Contractor:	M Technical Limited