CMIT Quality Policy and Procedures

8. Information and Data Management policy

College of Management and IT
Southern Cross Business Park
Bray, Co. Wicklow.

Updated: 12-Sep-23

8.1 Introduction

What is the purpose of this policy?

- A Data Protection and Privacy Policy is in place for the following reasons (1) to communicate the security measures CMIT undertakes to secure personal and commercial data, (2) to communicate the rights of individuals regarding data held and managed by CMIT, (3) to outline state CMIT's policies regarding the collection, storage, protection, and deletion of personal data, and (4) to convey that our data policies are compliant with GDPR and Data Protection regulations.
- To ensure that reliable information and data are available for informed decision-making and planning by the college.
- To ensure compliance with infrastructure, resources aspects of the Topic Specific Statutory Guidelines for providers of Blended Learning Programmes.

To whom does this policy apply?

- The policy applies to all staff, learners, and committee members of the college.

Who is responsible for implementing the policy?

- The Senior Management Team are responsible for the implementation of this policy.

Sections in this document

8.2 Learner Information System and Management information systems

Learner Information System

- CMIT utilises a robust and secure information system to record student information.
- The system is controlled and accessed only by authorised staff.
- The system records data necessary for learner to enrol and become certified in their course.
- The information system is used for compilation of Internal Verification, External Authentication reports and for uploading data to QQI's QBS system.
- The Learner Information Management System is robust, comprehensive, and capable of:
  - Maintaining secure learner records for current use and historical review.
  - Providing reports required for internal quality management and improvement
  - Generating data required for, and compatible with, external regulatory.
  - Professional or national systems as appropriate.
  - Generating statistical and other reports to meet internal and external information requirements, for example, on the QQI database of programmes and awards as prescribed by the legislation.
  - Ensuring that the database is maintained securely and that data relating to Learner assessment is accurate and complete.

- Reports which can be derived from the system include:
  - Enrolment data.
  - Learners contact information.
  - Learner progress.
  - Learner grades.
  - Results of Internal Verification.
  - Results of External Authentication.
  - Grade statistics.
  - Completion rates.

Management Information Systems

- CMIT uses a Management Information system to track organisation-wide performance metrics. Key metrics include:
  - Assessment quality (measured through grade changes by External Authenticators).
  - Learner Skill Transfer (measured through learner surveys).
  - Learner Satisfaction (measured through learner surveys).
  - Net Promoter Score (measured through learner surveys).
  - eLearning site uptime (measured through external monitoring).
  - Learner completion rates.

- CMIT also uses monthly audits to track compliance with operational quality issues.
- CMIT uses a tracker system to track progress with corrective actions.

8.3 Records Maintenance and Retention

Record keeping

- CMIT regularly purges databases of data, which is no longer needed, including personal data relating to learners or staff members.
- CMIT has a systematic process in place for the deletion of data from all systems and responsibility has been assigned for maintaining/deleting data.
- Data is classified to indicate the sensitivity level and the purpose associated with holding all data is defined.
- In compliance with GDPR, CMIT has clearly defined times for how various long types of data are to be retained. Retention times are based on: (1) the need to delete personal data as soon as the purpose for which we obtained the data has been completed. (2) the need to hold data to undertake our commercial function (i.e., training and education), and (3) the need to comply with regulatory requirements (e.g., tax, accounting, and accreditation body requirements).

Data security and controls

- **Staff training:** the policies and procedures outlined here are incorporated into company practice maintaining an elevated level of security awareness. The protection of sensitive data demands regular training of all employees and contractors. Periodic security awareness meetings are undertaken to incorporate these procedures into day-to-day company practice.
- **eLearning system security controls**: CMIT makes use of HTTPS/TLS security to verify that users are communicating with the correct server. HTTPS/TLS encrypts and verifies the integrity of traffic between the client and our servers. CMIT contract a certified Moodle Partner to manage our LMS. We use global Tier 3+ (99.982% uptime) data centres to host our sites. Security features deployed include penetration testing, firewalls, advanced fire/electrical/mechanical monitoring, network redundancy, brute force defence mechanisms, daily backups on the server, daily off-server backups, regular patch updates, and access monitoring.
- **Open website security controls**: CMIT's website makes use of HTTPS/TLS security to verify that users are communicating with the correct server. HTTPS/TLS encrypts and verifies the integrity of traffic between the client and our servers. We use global Tier 3+ (99.982% uptime) data centres to host our websites. Security features deployed include penetration testing, firewalls, advanced fire/electrical/mechanical monitoring, network redundancy, brute force defence

mechanisms, daily backups on the server, daily off-server backups, regular patch updates, and access monitoring.

- **Physical security**: CMIT has procedures for preventing unauthorised individuals from obtaining sensitive data in our physical locations, including alarm systems (sensor, contact, smoke, fire), CCTV, restricting visitor/contractor access, ensuring workstations and devices are encrypted, secure disposal of hardcopy paper documents and secure disposal of devices after use (including device shredding).
- **Network and PC security**: CMIT uses hardware and software firewalls to secure our resources. PC workstations/laptops/mobile devices and external drives are encrypted. Restrictions and controls are in place around software installation. Up to date enterprise-level anti-virus, malware and email scanning is in place.
- **Passwords and system access permissions**: Policies and procedures are in place to control each employee's access to device, networks, and systems. A range of protocols are in place to control access to including strong password design protocol, 2FA, forced password change, email verification, and audit logs.

8.4 Data Protection and Privacy policy

General Statement

- This statement is CMIT's Data Protection and Privacy Policy learners, prospective learners, and visitors to our online services.
- The statement is updated in line with changes in legislation, best practice, and actions taken by CMIT to improve data protection and privacy.

We will obtain and process information fairly

- CMIT fully respects the moral and legal rights of individuals to privacy and will not collect any personal information without their expressed permission.
- Any personal information which you volunteer will be treated with the highest standards of security and confidentiality, under **General Data Protection Regulation (2018).**

Agreement with policies

- Before commencing a course with CMIT, learners must formally accept with our Terms and Conditions.
- Prospective students and visitors to our websites, must click on a 'popup' button to accept the use of cookies.

We will keep information only for specified purposes and use and disclose it only in ways compatible with these purposes

- **Emails, messages, and form data**: Emails, messages and form data is used and stored by CMIT to assist in completion of a course or for marketing purposes. This data will be collected, stored, and communicated per the principles outlined in the Data Protection Acts. Emails, messages, and form data is deleted in line with our data retention policies.
- **Personal data**: CMIT collects personal data such as Name, Address, contact details, date of birth and PPS numbers to assist learners in competing a course and to facilitate certification with award bodies. This data will be collected, stored, and communicated per the principles outlined in the Data Protection Acts. CMIT will not provide this information to any third party, except for the accreditation body, who require this information for certification purposed. Accreditation bodies (such as QQI and ILM) may hold personal details (e.g., name, PPS, date of birth) indefinitely. Many award holders contact awarding body for verification of their

qualifications, for a variety of reasons, e.g., commencing new employment and proof of qualification to access a college programme. QQI provide additional guidance here. ILM provide additional guidance here.

- **Assessment documents**: All assessment work is uploaded securely to the CMIT eLearning platform, which is password protected and fully encrypted. Assessment data is only used and stored by CMIT for completion of a programme. We may retain anonymised assessments for the purpose of facilitating plagiarism checking. We may collect personal data to assist you in completing your programme. This data will be collected, stored, and communicated per the principles outlined in the Data Protection Acts. Assessment work is deleted in line with our data retention policies. Assessment data is only used and stored by CMIT for completion of your course, except for the following: (1) Learners agree that in the event of CMIT ceases to provide a QQI programme, which is three months or longer in duration, that learner data (including registration data and assessments) may be transferred to QQI or QQI registered organisations to assist in the completion of your programme. You may request for this information not to be transferred. However, this may result in you not completing your course and not receiving your certificate, and (2) where a course is paid for by a third party (such as an employer or funding body) on behalf of a learner, then learners agree that CMIT may provide information, if requested, by the third party, regarding participation on the course and submission of assessments, by the learner.
- **Tutor feedback:** Tutor feedback is stored for the purpose of assisting you complete your course and is not shared with any third parties.
- **Grades and programmes completed**: We keep learner records secure for their current use (e.g., assessment records for certification purposes) and historical review (e.g., to record that a learner has completed a programme). We also generate data required for, and compatible with, external regulatory, professional, or national systems as appropriate, for example reports to meet internal and external information requirements, for example, on the QQI database of programmes and awards as prescribed by the legislation. CMIT will not provide grade information to any third party, except for the accreditation body, who require this information for certification purposed.
- **Statistical data**: we also maintain aggregate statistical data which does not identify learners personally. Examples include minimum and maximum learner numbers per programme; profile of the learner population; learner satisfaction rates; learner progression/ learner attrition or drop-out rates/completion rates; graduation/certification rates and including grade analysis.
- **Website data:** If we collect information on a form, we will explain the purpose of the form and only use the data collected for that purpose. Data may also be anonymised and used for statistical purposes.
- **Cookies:** Our websites use "cookie" technology. CMIT uses two distinct types of cookies. "Session" cookies help users to navigate through our website. They are

deleted once you leave our website. Session cookies allows the webserver to "remember" where you are on the website. "Tracking" cookies: this website stores cookies on your computer. These cookies are used to collect information about how you interact with our website and allow us to remember you. We use this information to improve and customise your browsing experience and for analytics and metrics about our visitors both on this website and other media.

We will keep information accurate, complete, and up to date

- You have the right to rectify any inaccurate personal data held about you.

We will give you a copy of your data on request

- You have a right to obtain a copy of any personal data we hold about you, free of charge, in an electronic format.
- Any access request will be concluded within one month.

Your right to erasure

- You have the right to be forgotten, and we will erase any personal data held on request.
- Any queries concerning the above may be made through info@cmit.ie

Your right to object to direct marketing

- You have the right to object at any time to the use of personal data (e.g., email addresses) for marketing purposes.
- All marketing communications are opt-in and will contain the ability to opt-out at any time.
- Any queries concerning the above may be made to info@cmit.ie

Who do we share personal data with?

- We may share your data with relevant third parties, where necessary, concerning the completion of your course, assessment, or certification; for example, QQI and ILM.
- We never share personal data with others for marketing purposes.
- Occasionally, we may receive requests from third parties with authority to obtain disclosure of personal data, such as to check that we are complying with applicable law and regulation, to investigate an alleged crime, to establish, exercise or defend

legal rights. We will only fulfil requests for personal data where we are permitted to do so in accordance with applicable law or regulation.

We will retain only relevant information for no longer than necessary

- CMIT regularly purges databases of data, which is no longer needed, including personal data relating to learners or staff members.
- CMIT has clearly defined times for how various long types of data are to be retained. Retention times are based on: (1) the need to delete personal data as soon as the purpose for which we obtained the data has been completed. (2) the need to hold data to undertake our commercial function (i.e., training and education), and (3) the need to comply with regulatory requirements (e.g., tax, accounting, and accreditation body requirements).
- **Physical security**: CMIT has procedures for preventing unauthorised individuals from obtaining sensitive data in our physical locations, including alarm systems (sensor, contact, smoke, fire), CCTV, restricting visitor/contractor access, ensuring workstations and devices are encrypted, secure disposal of hardcopy paper documents and secure disposal of devices after use (including device shredding).
- **Network and PC security**: CMIT used hardware and software firewalls to secure our resources. PC workstations/laptops/mobile devices and external drives are encrypted. Restrictions and controls are in place around software installation. Up to date enterprise-level anti-virus, malware and email scanning is in place.
- **Passwords and system access permissions**: Policies and procedures are in place to control each employee's access to device, networks, and systems. A range of protocols are in place to control access to including strong password design protocol, 2FA, forced password change, email verification, audit logs.

Policy on use of online messaging

- Learners are provided with access to CMIT's online learning platform for the duration of their programme of study.
- Learners must comply with the following rules which govern the use of the system:
  - Not to distribute, disseminate, or store images, text or materials that might be considered indecent, pornographic, obscene, or illegal.
  - Not to make inappropriate use of others' personal information or post confidential information about another person.
- Not to distribute, disseminate, or store images, text or materials that might be considered discriminatory, offensive, or abusive, in that the context is a personal attack, sexist or racist, or might be considered as harassment.
- User Messages are monitored frequently for potential misuse.

Contact Information

- If you have any questions about this privacy statement or how and why we process personal data, please contact us at: Data Protection Officer, CMIT, Southern Cross Business Park, Bray, Co. Wicklow. Email: info@cmit.ie

How to exercise your rights

- **Access to personal data**: you have a right of access to personal data held by us. This right may be exercised by emailing us at info@cmit.ie. We will aim to respond to any requests for information promptly, and in any event within the legally required time limits (currently 30 days).
- **Amendment of personal data**: to update personal data submitted to us, you may email us at info@cmit.ie.or, where appropriate, contact us via the relevant website registration page or by amending the personal details held on relevant applications with which you registered. Once we are informed that any personal data processed by us is no longer accurate, we will make corrections (where appropriate) based on your updated information.
- **Withdrawal of consent**: where we process personal data based on consent, individuals have a right to withdraw consent at any time. We do not process personal data based on consent (as we can usually rely on another legal basis). To withdraw consent to our processing of your personal data please email us at info@cmit.ie.

Changes to this privacy statement

- We recognise that transparency is an ongoing responsibility so we will keep this privacy statement under regular review.