Document Name and Version	**3.8 Data Protection in Assessments**
Policy Number	3.8
Policies that Interact with Policy 3.8	Part 10: Data Protection
Approval Body	Academic Council
Date of Approval	February 2020
Date Policy Comes into Force	25th January 2021
Date of Review	2025
Revisions	

1. Preamble.

1.1 *Regulatory Compliance:* This policy addresses the requirements of (i) QQI's suite of QA guidelines, and (ii) ESG and (iii) General Data Protection Regulations [GDPR] through clarification of learner responsibilities in relation to personal information. This policy works with IICP College Data Protection suite of policies, which cover the responsibility of IICP College, staff and learners in relation to data protection.

1.2 This policy and procedure provide information to learners on how to gather and store personal information legally, responsibly and ethically.

1.3 The requirements outlined in these policies and procedures provide guidance on the required steps to take in order to ensure that personal information gathered for assessment purposes is gathered appropriately and is kept safe and secure. The appropriate processing of personal information is required under Data Protection legislation and is also a key ethical requirement for Counsellors and Psychotherapists.

1.4 This policy also provides guidance on what can be done in order to improve safety and security of personal data.

1.5 The responsibility for managing personal information legally and ethically lies with the person who collects, stores and/or uses this information. This may be a learner, teacher or other staff member. This policy is designed to assist learners to comply with data protection legislation when engaged in assessment activity that involves processing personal data.

1.6 This policy addresses the requirements of (i) QQI's suite of QA guidelines, and (ii) ESG. These regulations require that areas addressed in quality assurance documentation include Data Protection.

2. **Scope.**

2.1 This policy applies to all training programmes at IICP College. Additional requirements may attach to different courses. These additional requirements will be available in the programme handbook.

2.2 This policy applies to all formative, summative and diagnostic assessments undertaken in IICP College.

3. **Purpose.**

3.1 Learners in counselling and psychotherapy programmes may be required to collect and hold personal information for the purposes of their learning and assessment. This data may relate to peers, colleagues, teachers, supervisors and clients. This policy advises on how that data can be managed safely and with due regard to the privacy rights of the people involved.

3.2 The purpose of this policy is to create awareness about appropriate security measures that must be implemented as part of the legal and ethical use of personal information.

4. **Roles and responsibilities.**

4.1 The Academic Council is responsible for formally approving this policy and for overseeing its implementation and review.

4.2 Learners are responsible for making themselves aware of their responsibilities under this policy, and for adhering to these regulations.

4.3 All faculty and staff are responsible for upholding this policy, and for adhering to its procedures.

4.4 Breaches of this procedure will be dealt with under IICP College's Data Protection suite of policies.

5. Policy.

5.1 IICP College's Data Protection policy requires all staff and learners to protect the rights and privacy of individuals in accordance with the Data Protection legislation. This requires that all assessment material identifying living persons is kept safe and secure.

5.2 New technology for data storage is being developed all the time, and the principle is that every person dealing with personal information should satisfy himself or herself that the system they use is sufficiently safe and secure. This information can be quite specialised, and seeking assistance and advice can be helpful. IICP College can only offer support to learners for college-run technology services.

5.3 All staff and learners are required to avoid sending personal data via email or file transfer without sufficient password protection.

5.4 All staff and learners should note that sensitive personal information should be treated with extra care. Sensitive personal information, as defined by the General Data Protection Regulations [GDPR] relates to specific categories of information which relate to a person's:

- Racial or ethnic origin;
- Political opinions or religious or philosophical beliefs;
- Physical or mental health or condition;
- Sexual life;
- Criminal convictions or the alleged commission of an offence, any proceedings for an offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings;
- Trade union membership.

5.5 The following general rules apply:

5.5.1 **Before gathering personal information**: IICP College staff and learners should consider the security approaches they plan to use in terms of their adequacy in protecting the type of personal data that they intend to gather, store and use.

5.5.2 **Before transferring personal information between devices**: Prior to transferring personal information from one location to another (for example from a computer to a laptop, or from a camera to a storage device) staff and learners must consider the security risks associated with the storage device and decide whether the location is sufficiently secure.

5.5.3 **When the use for which the personal information was gathered is ended:** Care must be taken to ensure that personal data collected as part of an IICP College programme is destroyed when your programme ends. This is usually following receipt of your award certificate or withdrawal from the course, whichever is the earlier. However, there may be an agreement with a research participant or other data subject that changes this general rule – where for example there is consent to hold onto data for future publication. This is agreed in advance with the data subject at the time of receiving consent.

5.5.4 **When storing personal data:** All personal and sensitive data held electronically should, where possible, be stored in a fixed location rather than a portable device.

5.6 Some forms of storage and transfer of personal information are unacceptable. These include the following:

- Standard unencrypted email should never be used to transmit personal information. However, where due care is exercised, a password protected email address can be used to transfer a password protected file.
- Personal information should not be stored on a device that is not secure. At a minimum, password protection of relevant files should be used. Preferably, data should be stored on an encrypted device.
- Paper files should be kept in a locked cabinet that only the user has access to.
- In general, data that is available via remote access should not be copied to portable storage devices that may be stolen or lost (such as laptops or USB keys) unless these devices have adequate security.

6. Procedures.

6.1 Keeping Personal Information Secure: Principles.

6.1.1 In order to prevent private, personal information inadvertently being shared with people who have no right of access, all staff and learners must ensure that (i) the storage system used is secure and (ii) information is stored carefully and securely.

6.1.2 **Poor security in a storage system**. This can happen, for example, when: you do not use a password, your password is not strong enough, or you do not lock a filing cabinet.

6.1.3 **Storing data in the wrong place**. This can happen, for example, when: you email a document to the wrong recipient, you access personal data on a public computer; or you leave a paper file in a reception area or on a bus.

6.2 Keeping Personal Information Secure: Steps.

6.2.1 **Keeping computers and computer files secure**. This requires controlling access to folders and files through means such as password protection and/ or by encryption. Anonymization (removing personal information) and pseudonymization (using false names and changing contextual details) are also useful in helping avoid disclosure of sensitive data. However, it should be noted that these rarely produce complete security, as individuals can usually still be identified.

6.2.2 **Keeping Networks secure**. Ideally this involves firewall protection and anti-virus protection installed on every computer on a network. Most personal computers have some form of virus protections, so it is important to check the security of any system used for personal information. As a general rule sharing personal or sensitive data over a network should be avoided unless its security can be trusted.

6.2.3 **Keeping physical data secure.** This requires control of access to rooms and equipment where data (digital or physical) are held and avoiding transporting sensitive data unless encrypted.

6.3 Data Protection when recording interviews for research or assessment.

6.3.1 Before carrying out a recording, learners should ensure that the recording is justified for the purpose of their learning, that they have anticipated ethical issues that might arise with the recording, and that they have obtained the required consent.

6.3.2 Learners should advise participants (and are advised themselves) not to identify third parties on recordings without their prior consent. Participants need to be particularly careful of naming others where sensitive information is involved.

6.3.3 Learners should keep in mind, and should inform all parties in a recording, that no recording can ever be completely anonymous.

6.3.4 All transcripts should identify participants by a code rather than by name (i.e. pseudonymization). If the recording and/or transcript is lost, stolen or mislaid this will assist in protecting a participant's privacy.

6.3.5 Additional precautions are required to ensure security if an interview recording is stored on portable media.

6.3.6 If recordings are to be used in publications, and the data is not irreversibly anonymized, the consent for this use will be required on the consent form.

6.4 Data Protection when transcribing interviews.

6.4.1 Transcription should, where possible, be undertaken by the researchers. If transcription is carried out by someone other than the researchers (e.g. a transcription service or research assistant) participants must be informed of this and their specific consent sought.

6.5 Transfer and deletion of personal data held on recordings and transcripts.

6.5.1 **The following steps are required:**

- Transfer interview from the secure recording device to a password protected file on your secure (i.e. at least password protected) PC or other storage device.
- Once you have checked that the version you have transferred to the password protected file on your device works properly, remove fully the original recording from the recording device.
- Store your other secure storage device in a secure location for the duration of writing your assessment.
- Write the assignment within the shortest possible time.
- Submit the written assignment to Moodle, with a copy of the recording and/or transcript as described in instruction for that assessment. The informed consent agreement should be submitted in accordance with programme requirements.

- Delete the copy held in the password-protected file following receipt of your award certificate. At this stage all assessments are complete, and the data is no longer required. This may not be the case if you have received consent for use that specifies a date for destruction. This may occur, for example, if you are using recordings of interviews for research purposes.

7. Definitions

7.1 **Anonymization** is when information is changed so that a person cannot be connected to their data. One way to do this is by changing names (Pseudonymization) and removing contextual information (such as gender, location, age etc.). Full anonymization is when no-one (not even the person who collected and used the data) can identify the individuals to whom it relates, and it is not possible that any individual could be identified from the data or together with other information which is available. This is difficult to achieve, particularly in small communities. It is good practice to use changed names and minimise contextual markers anyway, even if this is not complete.

7.2 **Data protection** is the means by which the privacy rights of individuals are safeguarded in relation to the processing of their personal data.

7.3 **Data aggregation** is when information is presented in a summarized format that removes any indication of how individuals contributed to the summary. The principle here is that it is not possible to move from the summary back to individual contributions to the summary. Statistical information from large or medium sized groups, such as census data, is one example. Text as well as numbers can be aggregated – for example where themes from a number of interviews are identified and there is no code that allows individual contributions to be traced.

7.4 **Encrypted Data** is personal data that is protected through technological measures to ensure that the data is only accessible/readable by those with specified access.

7.5 A **firewall** is a product (software, hardware or both) that is attached to the Internet and a computer device. Firewalls use methods such as filtering and passwords to make sure that only those who are authorised can access a network.

7.6 **Internal and External networks.**

7.6.1 An external network allows access to multiple users. Most external networks have security such as encryption and firewalls. Some do not. Free access connections to the internet that may be available through coffee shops, transport networks or public spaces generally do not have sufficient security to allow you to access personal information. Storing personal information in an external network that has security is like leaving your valuables in your house – how secure they are depends on how good your locks and alarms are, and generally a house is secure enough. Storing personal information on an external network that has no security is like storing your valuables on the high street – everyone can access them.

7.6.2 An internal network, called an intranet, is one which is restricted to a defined set of users. An example would be a network accessed only by the learners of a specific college. Physically, an internal network is like a safe within a house, where only those with the key to the house and the access code to the safe can gain access to the valuables within it.

7.7 **Personal data** is data relating to a living individual who is or can be identified either from the data or, from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller. This can be a very wide definition depending on the circumstances.

7.8 **Pseudonymization** of data means that identifying information is removed from personal data. The data is not anonymized as there is a process that can be used (such as a key, or contextual information) to determine who is spoken about in the data. This is often used in research, where the person’s name is changed but the researcher keeps a record of the relationship between the real name and the pseudonym.

7.9 **Sensitive personal data** relates to specific categories of data which are defined as data relating to a person's:

- racial or ethnic origin;
- political opinions or religious or philosophical beliefs;
- physical or mental health or condition;
- sexual life;
- criminal convictions or the alleged commission of an offence, any proceedings for an offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings;
- trade union membership.

This Policy document will be reviewed regularly and updated as appropriate in line with any legislative or other relevant development.

8. **Supporting Documentation.** Please note: These forms may be adapted to fit with the requirements of particular modules, such as simulated role-plays. Please check with your lecturer before using.

8.1 Consent for use of Individual Client Session as Submission to Course for Review and Assessment purposes.

IICP College, Killinarden, offers a BA (Hons) Degree in Integrative Counselling and Psychotherapy and I am currently registered on this programme.

As part of the course requirements, I am required to complete a case study based on clinical work. This will include reviews of clinical sessions and may include recordings of same. This will be reviewed, for educational and clinical purposes, by course lecturers, the Course Director and may also be submitted to the External Examiner. All persons noted here are bound by the code of ethics of their accreditation bodies, and by the confidentiality policy of IICP College, so your identity will be protected and kept confidential at all times.

Case study assignments may also be used for publication purposes. Here, your right to confidentiality and anonymity are protected through the application of a pseudonym (false name), which will be applied at all times. Your name will not be written on the tapes or documents and your real name will not be used at any point beyond this consent form.

I commit to adhering to the Code of Ethics and Data Protection Policy of my accrediting body, as well as the IICP College code of behaviour and assessment strategies. Additionally, I consent to comply with all IICP College policies regarding the protection and storing of sensitive research data.

My therapist has informed me that they will delete all recordings once their programme is complete, in accordance with the College policy ☐

1. Do you agree to our client session(s) and information gathered in sessions utilised in a case study that will be submitted by me to meet with programme, academic and professional requirements? Yes, I consent ☐ No I do not consent ☐

2. Do you agree to our client session(s) being audio/video taped, transcribed and utilised in a case study that will be submitted by me to meet with programme, academic and professional requirements? Yes, I consent ☐ No I do not consent ☐

3. Sometimes case studies are considered for publication in academic journals or books. Do you agree to work included in the final submission being considered in reviewed format for publication? Yes, I consent ☐ No I do not consent ☐

You may withdraw your consent without prejudice up to: ____________________ (insert date).

Please sign in the space below to indicate confirmation of your informed consent to this case-study.

Date: ________________________

Signature of Client: ________________________

Signature of Therapist: ________________________

Copy of Consent Form to be given to Client