GENERAL DATA PROTECTION RULES

(GDPR) Guidelines

November 2018

STRICTLY CONFIDENTIAL

For internal/Client use only

Introduction

General Data Protection Regulation (hereafter referred to as GDPR) came into force on 25 May 2018. This Act is designed to protect the privacy of individuals.

This booklet specifically focuses on Counsellors, and Clients but applies to members of staff (if any) Data within Kairos Counselling Centre and the protection of this data.

Kairos Counselling Centre takes the privacy of our Clients and Counsellors seriously and wishes to deliver all the rights and entitlements under this act to our Counsellors and Clients to protect, safeguard and allow them access to their personal data. As a result, the following policies and processes have been developed, will be rolled out and the appropriate training will be provided to Counsellors:

As indicated above, these are contained within the pages of this booklet.

If you have any queries or questions regarding GDPR, Counsellor and Client data protection or accessing personal data, please contact Kairos Counselling Centre.

Counsellor and Client GDPR – Our Approach

Kairos Counselling Centre recognises that your privacy and data protection rights are very important to you, and to us. We want to support your privacy and your data by keeping them safe. Therefore, we pledge that all Counsellors and Clients personal data will be maintained in accordance with the obligations of the Data Protection Acts and GDPR.

Data Protection is the safeguarding of the privacy rights of Counsellors and Clients in relation to the processing of personal data, in both paper and electronic format.

The Data Protection Acts 1988 and 2003 (the "Data Protection Acts") and GDPR 2018 lay down strict rules about the way in which personal data and sensitive personal data are collected, accessed, used and disclosed. The Acts also permit Counsellors and Clients to access their personal data on request in writing and confer on Counsellors and Clients the right to have their personal data amended if found to be incorrect.

Data Protection Roles:

DPO (Data Protection Officer) – Member of the Management Team

DPC (Data Protection Controller) - Kairos Counselling Centre & Counsellors

DPP (Data Protection Processors) – Kairos Counselling Centre and Counsellors

DPS (Data Protection Subject/s) – Counsellors and Clients

This booklet outlines our policies regarding compliance and governance of Counsellor and Client data protection in keeping with the above.

Our Data Protection Commitment to you, our Counsellors and Clients

This is our commitment to protect the rights and privacy of Counsellors and Clients in accordance with the Data Protection Acts and GDPR when we collect, retain and store your data:

Collecting information

We collect and use Counsellor and Client information to provide the following services to and for you, our Counsellor and Client:

- To service the relationship and contract;
- To communicate with you regarding service related matters;
- To be compliant with Revenue, Social Welfare, Immigration, Work Approval rules and regulation as a Service provider with Counsellors;
- To provide a full range of database management services, including matrices, reporting and compliance and data validation and correction;
- To perform accounting and other record-keeping functions;
- To use your name and address data for identity verification, anti-fraud and anti-money laundering services.

Data Protection Principles

We shall perform our responsibilities under the Data Protection Acts in accordance with the following eight Data Protection principles:

- **Obtain and process information fairly**
  We will obtain and process Counsellor and Client personal data fairly and in accordance with statutory and other legal obligations.
- **Keep it only for one or more specified, explicit and lawful purposes**
  We will keep Counsellor and Client personal data for purposes that are specific, lawful and clearly stated. Personal data will only be processed in a manner compatible with these purposes.
- **Use and disclose only in ways compatible with these purposes**
  We will use and disclose personal data only in circumstances that are necessary for the purposes for which we collect the data.
- **Keep it safe and secure**
  We will take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of personal data and against its accidental loss or destruction.
- **Keep it accurate, complete and up-to-date**
  We adopt procedures that ensure high levels of data accuracy, completeness and up-to-date data.
- **Ensure it is adequate, relevant and not excessive**
  We endeavour to only hold personal data to the extent that it is adequate, relevant and not excessive and will retain the data for no longer than is necessary.

- **We have a retention policy for personal data**
  Give a copy of his/her personal data to that individual, on receiving a written request.
- **We will adopt our procedures to ensure that Counsellors and Clients can exercise their rights under the Data Protection legislation to access their data.**

Responsibility

The overall responsibility for ensuring compliance with Data Protection Acts rests with us. However, our responsibility varies depending upon whether we are acting as a Data Controller or a Data Processor.

All our Counsellors, Clients and contractors who separately collect, control or process the content and use of personal data are individually responsible for compliance with the Counsellor and Client Data Protection Acts.

Procedures and Guidelines

We are firmly committed to ensuring personal privacy and compliance with the Data Protection Acts, including the provision of best practice guidelines and procedures in relation to all aspects of Counsellor and Client Data Protection.

Review

This Data Protection Policy will be reviewed regularly considering any legislative or other relevant developments.

Kairos Counselling Centre 's Privacy Policy

This policy explains how we protect and manage Counsellor and Client personal data that we hold about you, including how we collect, process, protect and share that data.

Counsellor and Client Personal Data means any information that may be used to identify an individual, including, but not limited to, a first and last name, a home address or other physical address and an email address or other contact information, whether at work or at home.

How we obtain your personal data

Information provided by you - You provide us with personal data when you join us as a Counsellor, member of staff or Client. This data is obtained via forms, email and in conversations with us. This includes, but is not limited to: your name, address, date of birth, email address and bank account details. We use this information to manage and administer our contract with you as a Counsellor, member of staff or Client.

We may also obtain information contained in any correspondence you may have with us by post or by email. We currently do not record telephone conversations. We may obtain sensitive medical information directly from you or from our Occupational Medical Advisors. The provision of all this information is subject to you giving us express consent. If we do not have consent from you, then we may not be able to service our engagement contract with you. This means that the legal basis for Kairos Counselling Centre holding your data is in order to service a contract of engagement.

Information we share with other sources - We only share information with third parties for the servicing of the engagement contract. We also use third parties and/or public sources to obtain information about you, for example, to verify identity for garda vetting (for counsellors and members of staff only). This information, (including your name, address, email address, date of birth, etc.) as relevant to us, will only be shared with reputable third-parties that operate in accordance with the General Data Protection Regulation (GDPR).

How we use your personal data

We use your personal data to manage and administer your contract of engagement. We always undertake to protect your personal data, including any health and financial details, in a manner which is consistent with the General Data Protection Regulation (GDPR) concerning data protection. We will also take reasonable security measures to protect your personal data in storage.

Transferring of your personal data outside of the European Economic Area (EEA)

We do not currently transfer your personal data outside the EEA. If in the future we transfer your personal data, in accordance with the terms of our data Protection Policy, outside of the EEA, we will make sure that the receiving service provider agrees to provide the same or similar protection as we do and that they only use your personal data in accordance with our instructions.

How long do we keep information about you?

We keep information in line with the retention policy. That is during your engagement with us and for seven years after your engagement has ended with us to comply with all legal, statutory and regulatory obligations. In all cases our need to use your personal information will be reassessed on a regular basis and information which is no longer required will be securely disposed of.

Your rights as a data Subject

Subject access requests - the General Data Protection Regulator (GDPR) grants you, our Counsellor, member of staff and Client, the right to access data that we hold about you. This is referred to as a subject access request. We shall promptly, and certainly within one month (30 days) from the point of receiving the written request, provide you with the personal information required. Our formal response will include details of the personal data we hold about you.

Right to rectification - you have the right to obtain from us, without undue delay, the rectification of inaccurate personal data we are holding concerning you.

Right to reassure - you have the right to obtain from us the personal data concerning you without undue delay.

Notification obligation regarding rectification or removal of personal data or restriction of processing - we will communicate any rectification or removal of personal data or restriction of processing unless this proves impossible or involves disproportionate effort.

Right to data portability - you have the right to receive your personal data, which you have provided to us, in a structured, commonly used and machine-readable format and have the right to transmit this data to another controller, without hindrance from us.

Right to object - you have the right to object, on grounds relating to your situation, at any time to the processing of personal data concerning you.

Right to not be subject to decisions based solely on automated processing - we do not carry out any automated processing, which may lead to an automated decision based on your personal rights.

Accuracy of information

To provide the highest level of service possible to you, we endeavour to only keep accurate personal data about you. We take reasonable steps to ensure the accuracy of any personal data or sensitive information we obtain. We ensure that the source of any personal data or sensitive information is clear, and we carefully consider any challenges to the accuracy of the information. We also consider when it is necessary to update the information, such as name or address changes, and you can help us by informing us of these changes when they occur.

Important Information

Questions and queries - if you have any questions or queries which are not answered by this booklet or have any potential concerns about how we use the personal data we hold, please write to: Kairos Counselling Centre.

Complaints - please contact us by writing to: The Data Protection Controller, Kairos Counselling Centre.

Counsellor and Client Data Access Policy & Process

Purpose of this policy

This document outlines our Access Request Policy to help ensure that we comply with requests made by Counsellors, members of staff and Clients to access their data under the provisions of the Data Protection Acts.

Procedure

Counsellors, staff and Clients may make a request from us as follows:

- **Right to establish existence of personal data (Section 3 Data Protection Acts).** Under Section 3 of the Data Protection Acts, a Counsellor, staff member or Client may write to us asking what personal data we keep on him/her. We will respond within 30 days of receipt of the request, giving you a description of the data we hold on you and the purposes for which it is kept. Please make your request in writing to us at: The Data Controller, Kairos Counselling Centre stating that you are making your request under Section 3 of the Data Protection Acts. Please note that, before we respond to your request, we may require that you provide us with satisfactory evidence of your identity and address. We do not accept Section 3 requests via telephone, email or text message.

- **Making an Access Request.** Under Section 4 of the Data Protection Acts, you may receive a copy of your personal data held by us upon written request. To respond to you under a Section 4 request, we ask you to:

  - Complete the Data Access Request Form
  - Sign and Date the Data Access Request Form
  - Attach a photocopy of your proof of identity and address to the Data Access Request Form.
  - Post the Data Access Request Form to the Data Controller's Office.

  Please note that we reserve the right not to process and release data requested where you have not complied with the requirements of Section 4 of the Data Protection Acts, or if the request is not received in writing. **PLESE NOTE:** we do not accept access requests via telephone, email or text message.

Responding to your Access Request

Once we have received your fully completed Access Request Form, and your proof of identity and address, we shall respond to you within the statutory period of thirty (30) days. If you are not satisfied with the outcome of your access request, you are entitled to make a complaint to the Data Protection Commissioner who may investigate the matter for you.

Review

This Access Request Policy will be reviewed regularly considering any legislative or other relevant developments.

Data Protection Information Sheet

What is personal and sensitive data? Personal data is data which can be used to identify you. This may include your name, date of birth, address, telephone number etc. Sensitive personal data is information related to any of the following: racial or ethnic origin, sexual orientation, political opinions, religious beliefs, trade union membership, health, offences and/or convictions.

Where will Kairos Counselling Centre store my data? Your data will be stored mainly in Kairos Counselling Centre in a locked cabinet with limited access on a need to know only basis e.g. relevant Counselors, the data controller following requests from Clients of Kairos Counselling Centre and Payroll processors.

How will you use my data? Your data will primarily be used for providing you with engagement and in the case of staff members payroll services. We will also use anonymised data for the purposes of HR matrices and statistical monitoring.

Can I withhold my consent? Yes, but Kairos Counselling Centre will not be able to provide you with services.

What is a Data Controller? A Data Controller is responsible for your data and must make sure that your data is processed according to the law. For example, a Data Controller is responsible for making sure that the information held about you is accurate and that it is kept secure.

Why might you share my personal and sensitive personal data? Who will you share it with? We will only ever share your information, with your permission, for the purposes we have stated above or if required to do so by law.

Obtaining the information, we hold about you - You have a right to ask for a copy of your information and to correct any inaccuracies. Under the Data Protection Acts we are required to respond to your written request within 30 days.

Counsellor, staff member and Client Data Consent Agreement

Permission to store and process your data

To help us to provide engagement services to you, as our Counselor, staff member or Client, we will need to record your details. These details include personal and sensitive data as stated above.

To comply with the Data Protection Acts we ask for your permission to store and process your personal and sensitive data for this purpose. We agree to take all possible measures to secure your data, access to which will be limited and, on a need, to know only basis. We will keep your data in a secure location for a maximum of 7 years after your tenure has ended. Should we become aware of a data breach, you will be notified immediately.

You are entitled at any time to access the data that is held on you. To do so, please make a request in writing to the Data Protection Controller and you will be provided with a copy of your file within 30 days of your request.

Please note that where necessary, reference or information regarding 3rd parties will be redacted from the documents prior to being provided to you.

Consent

I give my consent to Kairos Counselling Centre for recording and retaining sensitive personal information about me for engagement purposes.

Name			
Signature		**Date**	

Counsellor and Client Data Access Request Form

This is a request for a copy of Personal Data under Section 4 of the Data Protection Acts. **Important:** proof of identity (e.g. passport or driver's licence) and a photocopy of proof of address (e.g. utility bill) must accompany this Access Request Form (see Note below).

Section A - please complete this section

Full Name_____

Postal address_____

Telephone/e-mail* (include area code) _____
* We may need to contact you to discuss your Access Request

Section B - please complete this section

I wish to have access to the following personal data (state request) _____

_____

Date_____

Checklist

Have you:

- completed, signed, and dated the Data Access Request Form? YES/NO
- attached a photocopy of proof of your identity and address? YES/NO

If you have ticked 'No' to any question above, we regret that we may not be in a position to provide you with the data requested. However, completing this form should enable us to process your request more efficiently.

Please return this form to:

- The Data Protection Controller (Counsellor or Kairos)
  or
- The Kairos Counselling Centre

We require proof of the applicant's identity and address to ensure that the person making this access request is acting legitimately.

Counsellor, staff and Client Personal Data Breach Procedure

Kairos Counselling Centre is obliged, under the Data Protection Acts, to keep personal data safe and secure and to respond promptly and appropriately to data security breaches (including reporting such breaches to the Data Protection Commissioner in certain cases). It is vital to take prompt action in the event of any actual, potential or suspected breaches of data security or confidentiality to avoid the risk of harm to our Counsellors, staff and Clients.

The purpose of this procedure is to provide a framework for reporting and managing data security breaches affecting Counsellors, staff and Clients' personal or sensitive personal data (defined above) held by Kairos Counselling Centre. These procedures are a supplement to the Kairos Counselling Centre's Data Protection Policy which affirms its commitment to protect the privacy rights of Counsellors, staff and Clients in accordance with Data Protection legislation.

WHAT IS A PERSONAL DATA SECURITY BREACH? A personal data security breach is any event that has the potential to affect the confidentiality, integrity or availability of personal data held by Kairos Counselling Centre in any format. Counsellor, staff and Client personal data security breaches can happen for several reasons, including:

- the disclosure of confidential data to unauthorised persons;
- loss or theft of data or equipment on which data is stored;
- loss or theft of paper records;
- inappropriate access controls allowing unauthorised use of information;
- suspected breach of Kairos Counselling Centre's IT security policies;
- attempts to gain unauthorised access to computer systems, e.g. hacking;
- records altered or deleted without authorisation by the Counsellor, staff or Client;
- viruses or other security attacks on IT equipment systems or networks;
- breaches of physical security e.g. forcing of doors or windows into secure room or filing cabinet containing confidential information;
- confidential information left unlocked in accessible areas;
- leaving IT equipment unattended when logged-in to a user account without locking the screen to stop others accessing information;
- emails containing personal or sensitive information sent in error to the wrong recipient;
- discussion of a Counsellor, staff and Client's data or situation with an unauthorised recipient.

WHO DO THESE PROCEDURES APPLY TO? These procedures apply to all users of Counsellor, staff and Client data, including:

- any person who is employed by Kairos Counselling Centre or is engaged by Kairos Counselling Centre who has access to Counsellor and Client data during their engagement or engagement for administrative, and/or any other purpose;
- members of Management team;
- any Counsellor, staff or Client of Kairos Counselling Centre who has access to personal data during their work for any purpose;

- Counsellors, staff or Clients who are not directly employed or engaged by Kairos Counselling Centre but who are employed by contractors (or subcontractors) and who may then have access to personal data during their duties for Kairos Counselling Centre.

WHAT TYPES OF DATA DO THESE PROCEDURES APPLY TO? These procedures apply to:

- all personal data created or received by Kairos Counselling Centre in any format (including paper records), whether used in the workplace, stored on portable devices and media, transported from the workplace physically or electronically or accessed remotely;
- personal data held on all Kairos Counselling Centre's IT systems managed centrally by the IT Dept, and locally by individual Departments/Offices/Functions or Centres;
- any other IT systems on which Kairos Counselling Centre data is held or processed.

WHO IS RESPONSIBLE FOR MANAGING PERSONAL DATA SECURITY BREACHES? Personal data security breaches are managed by the Data Controller's Office on behalf of the Data Controller.

Breaches

In the event of a breach of personal data security occurring, it is vital to ensure that it is dealt with immediately and appropriately to minimise the impact of the breach and prevent a recurrence. If an actual, potential or suspected breach of Counsellor, staff or Client personal data security occurs, the incident must be reported to the Data Controller's Office immediately.

The Data Controller must then:

- complete the Data Security Breach Report Form and email it to the Data Controller's office as soon as possible.

This will enable all the relevant details of the incident to be recorded consistently and communicated on a need-to-know basis to the relevant Counsellor, staff member or Client, so that prompt and appropriate action can be taken to resolve the incident.

PROCEDURE FOR MANAGING DATA SECURITY BREACHES. In line with best practice, the following five steps should be followed in responding to a data security breach:

Step 1: Identification and Initial Assessment;
Step 2: Containment and Recovery;
Step 3: Risk Assessment;
Step 4: Notification;
Step 5: Evaluation and Response.

Step 1: Identification and initial assessment of the incident

If a data security breach has occurred, this must be reported immediately to the Data Controller. The Data Controller should complete Part 1 of the Data Security Breach Report Form (Appendix 1) without delay. Part 1 of the Report Form will assist the Data Controller in conducting an initial assessment of the incident by establishing:

- if a Counsellor, staff member or Client personal data security breach has taken place; if so:
  - what personal data is involved in the breach;
  - the cause of the breach;
  - the extent of the breach (how many Counsellors, staff and Clients are affected);
  - the harm to affected Counsellors, staff and Clients that could potentially be caused by the breach;
  - how the breach can be contained.

Following this initial assessment of the incident, the Data Controller's Office will investigate the incident or appoint an Investigator. Any records relating directly to an investigation will be retained by the Data Controller's Office. The Investigator will determine the severity of the incident using the checklist in Appendix 2 and by completing part 2 of the Data Security Breach Report Form (Appendix 1) (i.e. will decide if the incident can be managed and controlled locally). The severity of the incident will be categorised as level 1, 2a, 2b or 3.

- Level 1 classed as a Local Incident;
- Level 2 (a) classed as a Minor Emergency Type (A) both managed and controlled locally;
- Level 2 (b) classed as Minor Emergency Type (B);
- Level 3 classed as a Major Emergency Escalated to Kairos management who will become responsible for the management and close-out of the incident.

Step 2: Containment and recovery

Once it has been established that a data breach has occurred, the Data Controller needs to take immediate and appropriate action to limit the breach. The Investigator, liaising with the Data Controller, will:

- Establish who, within Kairos Counselling Centre, needs to be made aware of the breach and inform them of what they are expected to do to contain the breach (e.g. isolating/closing a compromised section of the network, finding a lost piece of equipment, changing access codes on doors, etc.);
- Establish whether there is anything that can be done to recover any losses and limit the damage the breach can cause (e.g. physical recovery of equipment/records, the use of back-up tapes to restore lost/damaged data);
- Establish if it is appropriate to notify affected Counsellors and/or Clients immediately (e.g. where there is a high level of risk of serious harm to Counsellor and/or Clients); (see above 'breaches')
- Where appropriate (e.g. in cases involving theft or other criminal activity), inform the Gardaí.

Step 3: Risk Assessment

In assessing the risk arising from a data security breach, the Data Controller's Office is required to consider the potential adverse consequences for Counsellors and/or Clients, i.e. how likely are adverse consequences to materialise and, if so, how serious or substantial are they likely to be. The information provided at Stage 1 on the Data Security Breach Report Form will assist with this stage. The Investigator and Data Controller's Office will review the incident report to:

Assess the risks and consequences of the breach:

- Risks for Counsellors and/or Clients:
  - What are the potential adverse consequences for Counsellor and/or Client's?

- How serious or substantial are these consequences?
- How likely are they to happen?

- Risks for Kairos Counselling Centre:
  - Strategic & Operational
  - Compliance/Legal
  - Financial
  - Reputational
  - Continuity of Service Levels

- Determine, where appropriate, what further remedial action should be taken on the basis of the incident report to mitigate the impact of the breach and prevent repetition.

- The Investigator will prepare an incident report setting out (where applicable):
  - a summary of the security breach;
  - the people involved in the security breach (such as staff members, Counsellors, Clients, contractors, external clients);
  - details of the information, IT systems, equipment or devices involved in the security breach;
  - any information lost or compromised as a result of the incident;
  - how the breach occurred;
  - actions taken to resolve the breach;
  - impact of the security breach;
  - unrealised, potential consequences of the security breach;
  - possible courses of action to prevent a repetition of the security breach;
  - side effects, if any, of those courses of action;
  - recommendations for future actions and improvements in data protection as relevant to the incident.

The incident report will then be furnished to the Data Controller's Office. The risk registers will be updated. Any significant risks will be noted and recorded.

Step 4: Notification

Based on the evaluation of risks and consequences, the Data Controllers Office will determine whether it is necessary to notify the breach to others, for example:

- the Gardaí;
- Counsellor and/or Clients (data subjects) affected by the breach;
- Provincial Leadership Team of the Religious Sisters of Charity under whose auspices Kairos Counselling Centre operates;
- The Data Protection Commissioner;
- the insurers;
- bank or credit card companies;
- external advisers.

As well as deciding who to notify, the Data Controller must consider: What is the message that needs to be put across?

In each case, the notification should include as a minimum:

- a description of how and when the breach occurred;
- what data was involved;
- what action has been taken to respond to the risks posed by the breach.

When notifying Counsellors and/or Clients, the Data Controller's Office should give specific and clear advice on what steps they can take to protect themselves and what the Data Controller is willing to do to assist them. The Data Controller should also provide details of who they can contact for further information.

Notification should have a clear purpose, e.g.

- To enable Counsellors and/or Clients who may have been affected to take steps to protect themselves (e.g. by cancelling a credit card or changing a password).
- To allow regulatory bodies to perform their functions, provide advice and deal with complaints, etc.
- In accordance with the Data Protection Commissioner's Personal Data Security Breach Code of Practice, all incidents in which personal data has been put at risk should be reported to the Office of the Data Protection Commissioner ("ODPC") as soon as the Data Controller's Office becomes aware of the incident but at a maximum within 72 Hours of the breach - except when the full extent and consequences of the incident has been reported without delay directly to the affected data subject(s) and it affects no more than 100 data subjects and it does not include sensitive personal data or personal data of a financial nature.
- In case of doubt, the Data Controller (the DPC) should report the incident to the ODPC. Any contact with the Data Protection Commissioner should be made through the Data Controller's Office. Initial contact with the ODPC should be made by the Data Controller's Office within 72 hours of becoming aware of the breach, outlining the circumstances surrounding the incident.
- This initial contact may be by e-mail (preferred by the ODPC), or telephone and must not involve the communication of personal data.
- The ODPC will decide regarding the need for a detailed report and/or subsequent investigation based on the nature of the incident and the presence or otherwise of appropriate physical or technological security measures to protect the data. In cases where the decision is made by the Investigator and the data Controller's Office not to report a breach, a summary of the incident with an explanation of the basis for not informing the Data Protection Commissioner will be retained by the Data Controller.

Step 5: Evaluation and Response

After a data security breach, a review of the incident by the Data Controller will take place to ensure that the steps taken during the incident were appropriate and to identify areas that may need to be improved. All data security breach reports should be sent to the Data Controller's Office who will use these to compile a central record (log) of incidents. The Data Controller will report incidents Kairos Management at least on a quarterly basis, in order to identify lessons to be learned, patterns of incidents and evidence of weakness and exposures that need to be addressed. For each serious incident, the Investigator and Data Controller will conduct a review to consider the following:

- What action needs to be taken to reduce the risk of future breaches and minimise the impact?

- Whether policies, procedures or reporting lines need to be improved to increase the effectiveness of the response to the breach?
- Are there weak points in security controls that need to be strengthened?
- Are Counsellors and Clients aware of their responsibilities for information security and adequately trained?
- Is additional investment required to reduce exposure and, if so, what are the resource implications?

Counsellors and Clients Personal Data Security Breach Report Form

Please act promptly to report any data security breaches. If you discover a data security breach, please notify the Data Controller immediately.

Section 1: Notification of Data Security Breach to be completed by the person reporting the incident

Date incident was discovered:		
Date(s) of incident:		
Place of incident:		
Name of person reporting incident:		
Contact details of person reporting incident (email address, telephone number, address):		
Brief description of incident or details of the information lost:		
Number of Data Subjects affected, if known:		
Has any personal data been placed at risk? If, so please provide details		
Brief description of any action taken at the time of discovery:		
Received by, on behalf of Kairos Counselling Centre:		
On (date):		
Forwarded for action to:		
On (date):		

Section 2: Assessment of Severity

Details of the IT systems, equipment, devices, records involved in the security breach:	
Details of information lost:	
What is the nature of the information lost?	
How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT systems?	
Is the information unique? Will its loss have adverse operational, research, financial, legal, liability or reputational consequences for Kairos Counselling Centre or third parties?	
How many data subjects are affected?	
Is the data bound by any contractual security arrangements e.g. to research sponsors?	
What is the nature of the sensitivity of the data?	
Please provide details of any types of information that fall into any of the following categories:	
HIGH RISK personal data	
Sensitive personal data (as defined in the Data Protection Acts) relating to a living, identifiable individual's	
a) racial or ethnic origin;	
b) political opinions or religious or philosophical beliefs;	
c) membership of a trade union;	
d) physical or mental health or condition or sexual life;	
e) commission or alleged commission of any offence	
f) proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.	
Information that could be used to commit identity fraud, such as personal bank account	

and other financial information and national identifiers, such as Personal Public Service Numbers (PPSNs) and copies of passports and visas.	
Personal information relating to vulnerable adults and children.	
Detailed profiles of Counsellors and Clients, including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed.	
Spreadsheets of marks or grades obtained by Counsellors & Clients, information about individual cases of Counsellor and Client discipline or sensitive negotiations which could adversely affect Counsellors and Clients.	
Security information that would compromise the safety of Counsellors and Clients if disclosed. Category of incident (1, 2a, 2b or 3): Reported to DP Officer/FOI Officer on: If level 2b or level 3, date escalated by Lead Investigator to Kairos Counselling Centre.	

Action taken - To be completed by the Data Controller

Action taken by responsible officer/s:	
Was incident reported to Gardaí? Yes/No	
If YES, notified on (date):	
Follow up action required/recommended:	
Reported to DP on (date):	
Reported to Kairos Counselling Centre Management (details, dates):	
Notification to Data Protection Commissioner YES/NO If YES, notified on:	
Details:	
Notification to data subjects YES/NO If YES, notified on:	
Details:	
Notification to other external, regulator? YES/NO If YES, notified on:	
Details:	

Checklist for assessing severity of the Breach

How serious is the incident?	
Level 1: Local Incident:	
Is this a local incident?	Local incident = limited disruption to services, department, building or Kairos Counselling Centre; no serious threat to life, property or the environment; no threat to the Kairos Counselling Centre's image/reputation.
Can the consequences of the security breach, loss or unavailability of the asset be managed locally within normal operating procedures?	If so, manage the incident according to the Data Security Breach Management Procedure (this procedure).
Level 2a: Minor Emergency Type A – Unlikely to Escalate into a Major Emergency:	
Is this a Minor Emergency (type A)?	Minor Emergency (type A) = Disruption to the functioning capacity of a key Kairos Counselling Centre building or a key service. Situation or incident (actual or potential) which poses a threat to life, property or environment, at a minor level but may escalate to Type B.
Do containment and recovery require assistance from other members of staff within Kairos Counselling Centre or specialist support teams outside the Kairos Counselling Centre?	
Does the breach require a notification to Kairos Counselling Centre's senior managers?	If so, the Lead Investigator (liaising with the DP) will decide who else needs to assist or be made aware of the breach
Level 2b: Minor Emergency Type B or Level 3: Major Emergency	
Is this a major incident?	
Does containment and recovery, or the consequences of the loss or unavailability of the asset, require significant resources beyond normal operating procedures?	

The incident level is defined by:	
Does the incident need to be reported immediately to the Gardaí?	
How important an information asset is it to Kairos Counselling Centre business process or function?	
If the asset is a vital record, is it unique – once lost, lost forever? Will its loss have adverse financial legal, liability or reputational consequences e.g. evidential records required to defend Kairos Counselling Centres interests?	
Is it business-critical? Do you rely on access to this information asset or can you turn to reliable electronic copies or alternative manual processes e.g. paper files if the information asset is unavailable?	
How urgently would access need to be restored to an information asset to resume business? or, if a workaround will keep business moving in the short term, how long will it take to return to the required standard of service?	
Does the loss or breach of data security involve high risk personal data, i.e.: Sensitive personal data (as defined in the Data Protection Acts) relating to a living, identifiable individual's a) racial or ethnic origin; b) political opinions or religious or philosophical beliefs; c) membership of a trade union; d) physical or mental health or condition or sexual life; e) commission or alleged commission of any offence, or f) proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.	
Information that could be used to commit identity fraud such as personal bank account, other financial information and national identifiers, such as Personal Public Service Numbers (PPSNs) and copies of passports and	

visas;	
Personal information relating to vulnerable adults and children;	
Detailed profiles of Counsellors & Clients; including information about work performance, **or** personal life that would cause significant damage or distress to that person if disclosed.	
Spreadsheets of marks or grades obtained by Counsellors and/or Clients, information about individual cases of Counsellor and/or Client discipline or sensitive negotiations which could adversely affect Counsellors and/or Clients.	
Security information that would compromise the safety of Counsellors and/or Clients if disclosed.	