

# Information Governance Policies and Procedures

## Contents

Section A .....	2
Introduction .....	2
Aim and Purpose .....	2
Information Governance Framework Principles for Nikki Hutchinson .....	3
Section B .....	4
Privacy Notice: Use of information .....	4
Retention Schedule .....	5
Data Processing .....	8
Section C .....	10
Data Breach .....	10
Subject Access Request .....	10
Right to Erasure .....	11
Complaints .....	11
Safeguarding your privacy .....	11

# Information Governance Policies and Procedures

## Section A

### Introduction

Data held by Nikki Hutchinson will be held lawfully and for the retention periods set out in section B of this policy document.

This document refers to:

- Written Documents
- Spreadsheets
- Hardcopy case notes and files
- Database entries
- Images
- Recordings
- Emails
- Text messages

- Supervision notes
- Visits to the organisations website
- Social media communication

## **Aim and Purpose**

The purpose of this document is to ensure that Nikki Hutchinson has a framework that ensures the rights and freedom of individuals in relation to their personal data (Article1) and adheres to best practice in the management of client information and business records.

Information Governance sets out the way in which information is collated by an organisation is managed and ensures that any information collected;

- is the right information
- is in the right place
- at the right time
- with the right people
- for the right reasons

This is a live document and may be updated at any time to reflect changes in law or growth of the business, and therefore should be revisited regularly to check for any updates. Nikki Hutchinson is fully committed to ensuring clients privacy and data protection rights.

For the purpose of this policy Nikki Hutchinson is the named Data Protection Officer/Controller and Head of Organisation.

## **Information Governance Policies and Procedures**

### **Information Governance Framework Principles for Nikki Hutchinson**

1. Assessment needs for Information Governance (IG) Training have been identified and fully met, with a 75 minute GDPR CPD Course provided by the Clinical Hypnotherapy School ([www.clinicalhypnotherapyschool.com](http://www.clinicalhypnotherapyschool.com)) completed. Refresher training is completed every two years.
2. Any changes to the business processes and/or operations will be planned and will comply with the framework to ensure any risks to personal and sensitive information are minimised.
3. Any data collected is solely for the purpose of providing a person-centred service to an individual client.
4. The Caldicott Principles are used to provide guidance in best practice when handling personal data, alongside the ICO's Office Codes of Practice. (<https://www.igt.hscic.gov.uk/Caldicott2Principles.aspx>)
5. All technology [Microsoft Office products including Outlook] used to store or facilitate information and communication is maintained according to the Data Retention Policy for Nikki Hutchinson.
6. All records are identifiable, locatable, retrievable, and intelligible according to regulations

set out by GDPR.

7. It is the responsibility of the Data Controller to ensure sufficient resources are in place to prioritise adhering to Data Protection Legislation in the business.

9. Any electronic devices where personal or sensitive, confidential information is held will be password protected. Individual documents stored electronically will also contain individual passwords.

10. Procedures have been put in place to ensure the General Data Protection Regulations are met.

These can be found in section C.

## Information Governance Policies and Procedures

### Section B

Privacy Notice: Use of information

In accordance with this data retention schedule there may be occasions when data is not destroyed due to ongoing investigation, litigation or enquiry. The data will be deleted upon confirmation that it is no longer required.

On some occasions anonymised personal data will be retained whereby a client has provided a testimonial for use on the organisations website. When data is non-identifiable GDPR law is no longer applicable.

Nonidentifiable means that if this data was left on a bus, no one, including the data subject would be able to identify that this data was relating to them.

- Personal information is collated and stored in hardcopy in a locked filing cabinet behind a locked door.
- Any document containing personal data will state "Official--sensitive, private and confidential" clearly.
- All emails will contain a privacy statement.

Under the General Data Protection and Retention (2018) legislation, regarding how your personal data is processed, all individuals have;

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- the right not to be subject to automated decision--making including profiling.

Please note that Nikki Hutchinson does not use automated

decision-making tools, including profiling.

## Website visitors

When an individual visits [www.nikkihutchinson.co.uk](http://www.nikkihutchinson.co.uk), I use Google analytics who are considered a third party service, to collect information about what visitors do when they click on my website, e.g. which page they visit the most. Google analytics only collect non-identifiable data which means I or they cannot identify who is visiting. Nikki Hutchinson will always be transparent when it comes to collecting personal data and will be clear about how that data is processed.

## Webhealer

Webhealer published their GDPR compliant Privacy Policy and the address is [www.phdinteractive.co.uk/privacy](http://www.phdinteractive.co.uk/privacy). Webhealer have also received further reassurance from legal advisors about the Gmail Privacy Policy released last week. "This privacy notice is compliant with GDPR and has clearly been designed with GDPR in mind. The privacy notice will have been sent to all Gmail users within the EU and makes it quite clear that the rights extended by that policy apply across Google as a whole".

## Social Media

Nikki Hutchinson uses a third-party provider, Hootsuite, to manage its social media interactions. Any messages sent to the inbox of social media accounts are stored by Hootsuite and permanently deleted after three months. Their Privacy notice can be found here: <https://hootsuite.com/en-gb/legal/privacy#>.

# Information Governance Policies and Procedures

## Retention Schedule

Information Asset	Information Owner Asset	Retention	Trigger for Disposal
Email (including sent items)	Head of organisation	Annual review period every January, any remaining live data untouched until following review period.	End of retention period
Contact details held on mobile devices	Head of organisation	All entries to be deleted prior to decommissioning of mobile device or reissue of device.	End of retention period
Recordings	Head of organisation	5 years or earlier if consent is withdrawn.	End of retention period
Images taken	Head of organisation	5 years or earlier if consent is withdrawn.	End of retention period
Promotional materials	Head of organisation	Until superseded – Consent to be rechecked prior to reissue	End of retention period

Paper Diaries	Head of organisation	3 months from the period in which its use ends.	End of retention period
Policies	Head of Organisation	Until new policy has been put into place.	End of retention period

Nikki Hutchinson:

## Information Governance Policies and Procedures

Information Asset	Information Owner Asset	Retention	Trigger for Disposal
Client records including session notes, initial consultation notes and client overview form.	Head of organization	In accordance with NCH regulation End of retention notes, initial consultation notes 7 years after final treatment session period. and client overview form has ended. Child records should be held until after 25th birthday, or 26 <sup>th</sup> birthday if aged 17 when treatment ends.	End of retention period.
Safeguarding records	Head of organization	Head of organization In accordance with the current organization insurance policy, 5 years after final treatment session has ended, unless superseded by new insurance policy.	End of retention period.
Sat Nav records	Head of organization	All entries to be deleted prior to End of retention decommissioning of mobile device or reissue of device.	End of retention period.
Waiting lists	Head of organization	Annual review period every January, End of retention old waiting list destroyed and new waiting list developed with any remaining live data transferred	End of retention period.

		to new live document.	
--	--	-----------------------	--

## Information Governance Policies and Procedures

Information Asset	Information Owner Asset	Retention	Trigger for Disposal
Continual Professional Development.	Head of organisation	To be retained when worker is in service and until 8 years afterwards.	End of retention period
Worker supervision records	Head of organization \and workers and supervisors.	To be retained when worker is in service and until 8 years afterwards.	End of retention period
Service evaluation records	Head of rorganisation	Transfer to anonymised data within 6 months of collection.	End of retention period
Tax returns	Head of organisation	6 years from the end of the financial period to which pertain to.	End of retention period
Incident/Accident reports	Head of organisation	40 years from date report was closed.	End of retention period
Insurance policies	Head or organisation	40 years from date policy ended.	End of retention period
Complaints	Head or organisation	2 years from complaint being resolved	End of retention period
Right to Erasure Request	Head or organisation	8 years from request being submitted and completed.	End of retention period
Subject Access Request	Head or organisation	8 years alongside session notes, or plus 2 years from case closure if request is made after 6 years of storing data.	End of retention period

Hard copy data will be destroyed via a cross shredding machine owned by the organisation, electronic data will be permanently deleted.

## Information Governance Policies and Procedures

### Data Processing

#### What are the lawful basis for processing data at Nikki Hutchinson?

**Consent in relation to communication:** the individual has given clear consent for their data to be processed for the specific purpose/s detailed in the consent form stored in their personal file.

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

**This means that Nikki Hutchinson does not require consent to hold your data to provide a service but does require your consent to contact you for specific purposes. Participating in the service by attending more than one appointment implies that you agree with the Terms and Conditions provided to you at the commencement of service delivery.**

### Description of processing

The following is a broad description of the way this organisation/data controller processes personal information. Clients wishing to understand how their own personal information is processed may choose to read the FAQ's / Terms and Conditions for treatment document, which compliments the policies detailed here.

### Reasons/purposes for processing information

Nikki Hutchinson processes personal information to enable the provision of Psychotherapy, Hypnotherapy, Reflexology, Facial Reflexology, Aromatherapy Massage and Reiki, to advertise services and to maintain accounts and records.

### **Type/classes of information processed**

Nikki Hutchinson processes information relevant to the above reasons/purposes. This information may include:

## **Information Governance Policies and Procedures**

- personal details
- family, lifestyle and social circumstances
- goods and services
- financial details
- employment and education details

Nikki Hutchinson also processes sensitive classes of information that may include:

- physical or mental health details
- racial or ethnic origin
- religious or other beliefs of a similar nature
- offences and alleged offences

Nikki Hutchinson processes personal information about:

- clients
- suppliers
- business contacts
- professional advisers
- supervisors

## **Information Governance Policies and Procedures**

### **Section C Data Breach**

All personal and sensitive data held by Nikki Hutchinson is held securely. Electronic data stored on a computer is stored on a password protected computer, in password protected documents held on the C: Drive of the computer. This supports the ability to retrieve data in the event of faults. Hardcopy data is held securely in a locked cabinet behind a locked door.

In the case of a data breach Nikki Hutchinson shall comply with the regulations set out under Article 33 of the GDPR;

1. In the case of a personal data breach, the data controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the ICO, unless the personal data breach is unlikely to result in a risk to



the rights and freedoms of the individual. Where the notification to the ICO is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The notification referred to in paragraph 1 shall at least:

- (a) describe the nature of the personal data breach including where possible, the approximate number of data subjects concerned and the categories (e.g. sessions notes, phone numbers) and approximate number of personal data records concerned;
- (b) communicate the name and contact details of the data controller where more information can be obtained;
- (c) describe the likely consequences of the personal data breach;
- (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

6. In the event that a data breach will likely cause a risk to the rights and freedoms of client data, the data controller must communicate the nature of the breach in clear, concise and plain language, to the client/s involved, without delay.

7. If a breach occurs but the data controller has gone to appropriate lengths to protect the data held on the client (e.g. password encryption of electronic files), or if the data controller has taken subsequent action to prevent the risk (e.g. immediately blocking a mobile device) then notifying the client will not be required.

### **Subject Access Request**

A Subject Access Requests (SAR) permits individuals to request a copy of their personal information.

## **Information Governance Policies and Procedures**

A SAR must be acted upon within one month, at the most within two months, any longer and reasonable reason must be provided. There are no fees unless there is a disproportionate fee to the organisation for sending out the information. Application for SAR should be held alongside session records, unless application was made after six years of the end of treatment. In which case the SAR will be held for a further two years after closure of SAR.

A SAR request will include information we hold about you, Nikki Hutchinson will:

- give you a description of it;

- tell you why we are holding it;
- tell you who it could be disclosed to; and
- let you have a copy of the information in an intelligible form.

SAR requests should be put in writing to Nikki Hutchinson. A response may be provided informally over the telephone with your agreement, or formally by letter or email. If any information held is noted to be incorrect an individual can request a correction be made to their own personal information. This should be made in writing to Nikki Hutchinson.

### **Right to Erasure**

Any person may put in a request for their personal data to be removed (the 'right to be forgotten' or the 'right to erasure'). In this instance hard copy data will be shredded using a cross shredding machine owned by the organisation and any electronic data will be permanently deleted. The client will be notified of the completion. The request for deletion of data and the confirmation of completion will be held securely until eight years after the request was made.

### **Complaints**

Nikki Hutchinson hopes to meet the highest quality standards when processing personal and sensitive data. Complaints can help identify areas for improvement and therefore Nikki Hutchinson would welcome you raising any concerns you have.

These Information Governance Policy documents were created to be as transparent and understandable as possible. It will not be completely exhaustive of all aspects of data collection. If you would like further information about a specific process, please contact Nikki Hutchinson.

If you feel you would like to make a complaint about how your personal and sensitive data is handled by Nikki Hutchinson you can contact Nikki Hutchinson directly. In the event that Nikki Hutchinson cannot resolve your complaint to your satisfaction you can contact the Information Commissioners Office on 0303 123 1113.

### **Safeguarding your privacy**

In the event of my death or sudden illness, my supervisor will contact existing clients and archive any client files in accordance with General Data Protection Regulations.