LEEDS HYPNOTHERAPY ACADEMY

General Data Protection Regulation (GDPR) Policy

Leeds Hypnotherapy Academy
201 Town Street. Leeds. LS10 3SN
0113 2709385 leedshypnotherapyacademy@gmail.com

Policy title	General Data Protection Regulation (GDPR) Policy
Version	1.0
Date of approval	05 October 2018
Policy supersedes	NA
Lead Director	Nigel A Franks Managing Director
Policy Lead (and author if different)	Nigel A Franks Managing Director
Name of any responsible group or committee	NA
Date issued	05 October 2018
Review date	October 2020
Target audience	All Leeds Hypnotherapy Staff and Consultants

Contents

Staff summary

Leeds Hypnotherapy Academy (LHA) is committed to conducting its functions in accordance with Data Protection laws and regulations and with the highest standards of ethical conduct.

This policy defines expected behaviours of staff and consultants in relation to the collection, use, retention, transfer, disclosure and destruction of personal data.

This policy is in line with the new General Data Protection Regulations (GDPR) 2018.

Personal data is information (including opinions and intentions) relating to an identified or identifiable natural person and is subject to legal safeguards and regulations restricting how organisations may process personal data.

Organisations handling personal data and making decisions about its use are known as data controllers. LHA as a data controller, is responsible for ensuring compliance with the data protection requirements outlined in this policy. Non-compliance may expose LHA to complaints, regulatory action, fines and or repetitional damage.

LHA is committed to ensuring effective implementation of this policy and expects all its staff and consultants to share in this commitment. Breaches of this policy will be taken seriously and may result in disciplinary action.

1 Purpose

This policy applies to all information where a Data Subject's Personal data is processed.

- in the context of the business activities of LHA;
- for the provision of services to individuals (clients, patients & students);
- to actively monitor the behaviour of individuals.

This policy applies to processing of personal data in electronic form (including electronic mail and documents created with electronic software) or where it is held in manual files that are structured in a way that allows ready access to information about individuals.

2 Background & context

Data protection legislation is linked with the Freedom of Information and the Human Rights Act. The focus of the Data Protection Act is on promotion of the rights of living individuals in respect of their privacy and the right to security and confidentiality of their data. It applies to all person identifiable data, whether held electronically or manually. The responsibility to maintain the confidentiality of that data resides with LHA, even if an agent or subcontractor processes that data.

Data protection legislation does not guarantee personal privacy at all costs but aims to strike a balance between the rights of individuals and the sometimes competing interests of those with legitimate reasons for using person identifiable data.

LHA is obliged to register all processing activities with the Information Commissioner's Office annually and failure to comply with this requirement is a criminal offence.

3 Definitions

Data Subject

The identified of identifiable natural person to which the data refers.

Identifiable Natural person

Anyone identifiably directly or indirectly in particular by reference to an identifier such as a name, identification number, location data, online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Data Controller

A natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of the processing of personal data.

Data Processor

A natural or legal person, public authority, agency or other body which processes personal data on behalf of a data controller.

Consent

Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Special Categories of Data Protection

Data pertaining to or revealing racial, or ethnic origin, political opinions, religious or philosophical beliefs, trades-union membership, data concerning health or sex life and sexual orientation, genetic and biometric data.

Process, Processed & Processing

Any operation or set of operations performed on personal data or on sets of personal data, whether by automated means or not.

Operations performed may include collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Protection

The process of safeguarding personal data from unauthorised or unlawful disclosure, access, alteration, processing, transfer or destruction.

Data Protection Authority

An independent public authority responsible for monitoring the application of the relevant data protection regulations set out in law.

Third Country

Any country not recognised as having an adequate level of legal protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Profiling

Any form of automated processing of personal data where personal data is used to evaluate specific or general characteristics relating to an identifiable natural, person. In particular to analyse or predict certain aspects concerning that natural person's performance at work, economic situations, health, personal preferences, interests, reliability, behaviours locations or movement.

Binding Corporate Rules

The personal data protection policies used for the transfer of personal data to one or more third countries within a group of undertakings or a group of enterprises engaged in a joint economic activity.

Encryption

The process of converting information or data into code to prevent unauthorised access.

Pseudonymisation

Data amended in such a way so no individuals can be identified from that data (whether directly or indirectly) without a "key" that allows the data to be re identified.

Anonymisation

Data amended in such a way that no individuals can be identified from that data (whether directly or indirectly) by any means or by any person.

4 Policy Effect

Information Governance Manager

LHA has its Information Governance managed through the Director in relation to data protection and Freedom of Information legislation.

Data protection by Design

To ensure all data protection requirements are identified and addressed when designing new systems or processes and or when reviewing or expanding existing systems or processes, each of them must be approved first before continuing.

A Data Protection Impact Assessment (DPIA) must be conducted for new and reviewed systems and processes. All DPIAs will be carried out by the Director and subsequent findings of the DPIA will be reviewed and approved or not.

Data Protection Principles

LHA has adopted the following principles to govern its collection, use, retention, transfer, disclosure and destruction of personal data.

Principle 1: Lawfulness, Fairness & Transparency

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. This means LHA must tell data subjects what processing will occur (transparency), the processing must match the description given to the data subject (fairness) and it must be for one of the purposes specified in the applicable data protection regulation (lawfulness). These processes will be made clear by our information to data subjects.

Principle 2: Purpose Limitation

Personal data shall be collected for specified and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means LHA must specify exactly what the personal data collected will be used for and limit the processing of that personal data to only what is necessary to see the specified purpose.

Principle 3: Data Minimisation

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed. This means LHA must not store any personal data beyond that which is strictly required.

Principle 4: Accuracy

Personal data shall be accurate and kept up to date. This means that LHA must have in place processes for identifying and addressing out of date, incorrect and redundant personal data.

Principle 5: Storage Limitation

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. This means LHA must wherever possible, store personal data in a way that limits or prevents identification of the data subject.

Principle 6: Integrity

Personal data shall be processed in a manner that ensures appropriate security of the persona data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. LHA must use appropriate technical and organisational measures to ensure the integrity and confidentiality or personal data is maintained at all times.

Principle 7: Accountability

The data controller shall be responsible for and be able to demonstrate compliance. This means LHA must demonstrate that the Six Data Protection Principles noted above are met for all personal data for which it is responsible.

Data Quality

- correcting personal data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the data subject does not request rectification;
- keeping personal data only for the period necessary to satisfy the permitted uses or applicable statutory retention period;
- the removal of personal data if in violation of any data protection principle of if the personal data is no longer required;
- restriction, rather than deletion of personal data insofar as:

    1. a law prohibits erasure;
    2. erasure would impair the legitimate interests of the data subject;
    3. the data subject disputes that their personal data is correct and it cannot be clearly ascertained whether their information os correct or incorrect.

Data Retention

To ensure fair processing, personal data will not be retained by LHA for longer than necessary in relation to then purposes for which it was originally collected or from which it was further processed.

The length of time for which LHA needs to retain personal data is dictated by statutes and governing body directive. The Data Protection Act says records are to be kept for no longer than necessary (though this period is not defined). The core purpose of the Act was to stop people abusing data held and using it for unethical purposes. There is a human right of an employer or business human right (protected by law), to maintain a livelihood.

It is a condition of your insurance policies (Contract Law) that records be kept for at least 7 years. Statutes of limitation (Under Civil Law or Tort) extend the possibility of an action against you beyond the time limits of the data protection act and your policy conditions. On this basis LHA will retain client, patient, student and staff records indefinitely, particularly those for minors. This will apply even when the patient is referred on, or if LHA ceases to trade. Although in most cases the

statute of limitation that applies for late discovered situations leading to an allegation of negligence is 3 or 6 years from the date that the patient discovers a problem, there are certain situations where the limitation period could be much longer.

Personal data should be destroyed as soon as possible when it has been confirmed that there is no longer a need to retain it.

Data Protection

The LHA will adopt physical, technical and organisational measures to ensure the security of personal data so much as is reasonably practicable. This includes the prevention of loss or damage, unauthorised alteration, access or processing and other risks to which it may be exposed by virtue of human action or the physical or natural environment.

- prevent unauthorised persons from gaining access to data processing systems in which personal data is stored, if a third party for example a web based host fails to maintain security this will be the responsibility of the third party and not LHA;
- prevent persons entitled to use a data processing system from accessing personal data beyond their needs and authorisation;
- ensure personal data in the course of electronic transmission during transport cannot be read, copied, modified or removed without authorisation;
- ensure that data its processed in accordance with this policy;
- ensure personal data is protected against undesired destruction or loss so far as is reasonably practicable;
- ensure that personal data collected for different purposes can and is processed separately;
- ensure personal data is kept no longer than necessary.

Subject Access Requests

Subjects have the right to access their personal data related to:

- information access;
- objection to processing;
- objection to automated decision making and profiling;
- restriction of processing;
- data portability;
- data rectification;
- data erasure.

If a person makes a request relating to any of the rights listed above then each request will be considered in accordance with all applicable data protection laws and regulations.

No administration fee will be charged for considering and or complying with such requests unless the request is deemed to be unnecessary or excessive in nature.

Data subjects are entitled to obtain (based upon a request made in writing to the LHA and upon successful verification of their identity), the following information about their own personal data:

- the purpose of the collection, processing, use and storage of their personal data;
- the source(s) of their personal data, if not obtained from the data subject;
- the categories of personal data stored for the data subject;
- the recipients or categories of recipients to whom the personal data has been or may be transmitted, along with locations of those recipients;
- the envisaged period of storage for the personal data or the rationale for determining the storage period;
- the use of any automated decision making, including profiling;

The data subject has the right to:

- object to the processing of their personal data;
- lodge a complaint with the Data Protection Authority;
- request rectification or erasure of their personal data;
- request restriction of processing of their personal data.

All requests for access to or rectification of personal data must be directed to LHA, who will record each request as it is received. A response to each request will be provided within 30 days of the receipt of the written request from the data subject. Appropriate verification must confirm that the requestor is the data subject or their authorised legal representative.

If LHA cannot respond fully to the request within 30 days, it shall nevertheless provide the following information to the data subject or the authorised legal representative within the specified time.

- an acknowledgement of receipt of the request;
- any information located it today;
- details of any requested information or modifications which will not be provided to the data subject, the reason(s) for the refusal and any procedures available for appealing the decision;
- an estimated date by which any remaining responses will be provided;
- an estimate of any costs to be paid by the data subject (e.g. where the request is excessive in nature).

It should be noted that situations may arise where providing the information requested by a data subject would disclose personal data about another individual.

In such cases LHA will redact or withhold information as may be necessary or appropriate to protect that persons rights.

Law Enforcement Requests & Disclosures

In certain circumstances it is permitted that personal data be shared without the knowledge or consent of the data subject. This is the case where the disclosure of personal data is necessary for any of the following purposes:

- prevention or detection of a crime;
- apprehension or prosecution of offenders;
- assessment or collection of a tax or duty;
- by order of a court or by any rule of law.

If a staff member receives a request from a court or any regulatory or law enforcement authority the Director must be informed immediately.

Transfers to Third Parties

LHA will only transfer personal data to or allow access by, third parties when it is assured that the information will be processed legitimately and protected appropriately by the recipient. Where third party processing takes place LHA will first identify if, under applicable law, the third party is considered a data controller or a data processor of the personal data being transferred.

Where the third party is a data controller, LHA will enter into an appropriate agreement with the controller to clarify each party's responsibilities in respect of the personal data transferred.

Where the third party is deemed to be a data processor, LHA will enter in to an adequate processing agreement with the data processor. The agreement must require the data processor to protect the personal data from further disclosure and only to process personal data in compliance with LHA instructions.

In addition, the agreement will require the data processor to implement appropriate technical and organisational measures to protect the personal data as well as procedures for providing notification off personal data breaches.

Should LHA outsource its services to a third party (including web and Cloud based services), LHA will identify whether the third party will process personal data on its behalf and whether the outsourcing will entail any third country transfers of personal data. In either case it will make sure to include adequate provisions in the outsourcing agreement for such processing and a third country transfers. LHA shall conduct annual audits of processing of personal data performed by third parties, especially in respect of technical and organisational measures they have in place. Any major deficiencies identified will be reported to and monitored by the LHA.

Complaints Handling

Data subjects with a complaint about the processing of their personal data should put forward the matter in writing to LHA. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case.

LHA will inform the data subject of the progress and outcome of the complaint within a reasonable period.

If the issue cannot be resolved through consultation between the data subject and LHA, then the data subject may, at their option seek redress through mediation, binding arbitration, litigation or a complaint to the Data Protection Authority.

Breach Reporting

If It is suspected that a data breach has occurred this must be notified immediately to the Director.

The Director will investigate all reported incidents to confirm whether or not a personal data breach has occurred. If a personal data breach is confirmed LHA will consider the criticality of the breach and the quantity of personal data involved. For severe personal data breaches there will be an emergency response to coordinate and manage the personal data breach response.

Relevant Legislation, Statutory Duties & Guidance

This is a summary of legislation relevant to the protection and use person identifiable information. All staff should be aware of their responsibilities under this legislation and have due regard for the law when collecting, using or disclosing confidential information.

Data Protection Act 1998:

This gives people the right:

- of privacy;
- to know the purpose for which their data is being held and processed;
- to know who their data may be disclosed to;
- of access to their data;
- to prevent the use of their data in certain circumstances.

It places legal obligations on everyone processing personal data and has eight data protection principles that must be complied with to protect data in accordance with the law.

There are a number of criminal offences by which staff may be prosecuted:

- processing person identifiable data without notifying the Information Commissioner;
- processing person identifiable data for any purpose over than that covered by agreement;
- unauthorised disclosure of person identifiable data e.g. disclosure to a person or organisation not entitled to receive it;
- failure to comply with an Information Enforcement notice issued by the Information Commissioner;
- modifying personal data subject to a subject access request;

- breaches of section 55 of the Data Protection Act (knowingly or recklessly disclosing information).

Computer Misue Act 1990

It is It illegal to access data or computer programs without authorisation. This act establishes three offence. It is illegal to:

- access data or programmes held on a computer without authorisation e.g. view client, patient, student or employee data when you are not directly involved in their care or management or obtain and view information about friends and relatives. On conviction an offender is liable to a custodial sentence of six months and fines of up to £2000 or both;
- access data or programs held on a computer without authorisation with the intention of committing further offences e.g. fraud or blackmail. On conviction an offender is liable to a custodial sentence of up to 5 years and fines of up to £5000 or both;
- modify data or programs held on a computer without authorisation. On conviction and offender is liable joint custodial sentence of up to 5 years and find up to £5000 or both.

Human Rights Act 1998

Two articles under this act are relevant to the confidentiality of person identifiable data:

- Article 8: Right to respect and family life;
- Article 10: Freedom of expression and exchange of information and opinions.

These articles relate to preventing disclosure of information received in confidence.

Freedom of Information Act 2006 - section 251

This section makes it lawful to disclose and use confidential patient information in specified circumstances where it is not currently practicable to satisfy the common-law confidentiality obligations.

Common Law Duty of Confidence

The basic principle is that information is confidential to the client, patient, student or employee and should not generally be disclosed without consent, unless justified for a lawful purpose or required by statute.

Every member of staff is responsible for ensuring that:

- patient, client, student and staff information is only used for specified and lawful purposes and that confidentiality is respected;
- they understand and comply with the law and if in doubt seek advice from the director.

Person identifiable information may be in any form including but not restricted to the following:

- paper records or documents;
- computer records or printouts;
- fax messages;
- telephone conversations;
- emails and attachments;
- CDs, memory sticks and other portable media;

5. Roles and Responsibilities

All staff working on behalf of LHA, involved in the receipt, handling our communication of personal identifiable data must adhere to this policy. Any stuff having concern or is not confident in what they are undertaking or witnessing should inform the Director.

All staff are expected to read this policy and recognise that they have a duty to respect the data subject's rights to confidentiality and to understand that disciplinary action and penalties could be imposed for non-compliance with this policy.

LHA is responsible for ensuring that all staff are informed of this policy and any changes to it. LHA is responsible for ensuring staff are aware of its policies and procedures and that they are adhered to.

6. Equality Analysis

LHA has assessed this policy for its impact upon equality (annex 1) and is committed to ensuring that services are provided our staff are treated reflecting individual needs and promoting equality without discriminating unfairly against any individual or group.

7. Consultation and Review Process

This policy will be disseminated to all staff by the Director.

8. Monitoring Key Performance Indicators

Compliance is measured by ensuring all aspects of the policy are met.

10. References & Associated Documents

- Copyright Designs and Patents Act 1988;
- Freedom of Information and Environmental Information Act 2000;
- Privacy and Electronic Communications Regulations 2000;
- Data Protection Act 1998;
- Computer Misuse Act 1980;
- Access to Health Records Act 1990;
- Access to Medical Records Act 1988;
- Human Rights Act 1998;

- Health Act 2009;
- Health and Social Care Act 2015;
- Data Retention and Investigatory Powers Act 2014.

Appendix A
Data protection principles

1. personal data shall be processed fairly and lawfully and in particular shall not be processed unless:

   a. at least one of the conditions in note 2 below is met;
   b. in the case of sensitive personal data, at least one of the conditions in schedule three is also met.

2. personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;
3. personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed,
4. personal data shall be accurate and where necessary kept up-to-date;
5. personal data processed for any purpose shall not be kept longer than is necessary for that purpose or those purposes;
6. personal data shall be processed in accordance with the rights of data subjects under this Act;
7. appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of personal data;
8. personal data shall not be transferred to any country or territory outside the European Economic Area unless the country or territory ensure an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Appendix B
Subject access request procedure

The data subject has rights under section 7 of the Act whereby they can request:

- confirmation that personal data relating to them is held by LHA;
- confirmation of the purpose(s) for processing personal data;
- a permanent copy of the personal data in hardcopy unless otherwise agreed;

Data subjects have the right to review and obtain a copy of all personal data about themselves that is held in computerised or manual formats irrespective of when they were created. To exercise this right individuals must make a written request for information where they are the subject of that information or data. If applying for access to a deceased persons records the Access to Health Records Act 1990 applies.

Rights of Subject Access

An application for data subject access request may be made by:

- **The data subject**
  is entitled to make a request in writing to see any personal data held about them under the act;
- **On behalf of the data subject**
  anyone applying for data subject access on behalf of someone else must apply in writing together with written authorisation from the data subject which must be signed by the data subject themselves;

- **A person with parental responsibility**
  a person can only request access if they have either a parental responsibility or a legal guardianship of the child. Parental responsibility is defined in the Children Act 1989 and updated by the Adoption and Children Act 2002. The individual(s) with parental responsibility must be acting in the best interests of the data subject (child). A person with parental responsibility is:

  a. the natural mother;
  b. the natural father, if married to the mother either before or after the birth, even if divorced or separated;
  c. the natural father, if un married, and he registered the birth along with the mother after December 2003;
  d. the natural father, if un married, by agreement with the mother, (evidenced by a form provided by a solicitor, signed by both parents and witnessed by an officer of the court) or by a court order (parental responsibility order);
  e. the natural father, if un married and appointed as the child's guardian on the death of the natural mother;
  f. an individual (generally a family member) with a residence order for the child (if the order is for a period of time, then parental responsibility is removed at the end of the period);
  g. an individual who has legally adopted child;
  h. a local authority under a care order - individual acting as children's guardian.

Requests for information about children

Even if a child is too young to understand the implications of subject access rights it is still the right of the child rather than of anyone else such as a parent or guardian. So it is the child who has a right to access the information held about them, even though in the case of young children those rights are likely to be exercised by those with parental responsibility for them.

Before responding to a subject access request for information held about child LHA will consider whether child is mature enough to understand their rights. If LHA is confident that the child can understand their rights then LHA will usually respond directly to the child. LHA may however allow the parent to exercise the child's rights on their behalf if the child authorises this or if it is evident that this is in the best interests of the child.

What matters is that the child is able to understand (in broad terms), what it means to make a subject access request and how to interpret information they receive as a result of doing so. When considering borderline cases account will be taken of, among other things:

- the child's level of maturity and their ability to make such decisions;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child;
- any consequences of allowing those with parental responsibility access to the child's personal data. This is particularly important if there have been allegations of abuse or ill-treatment;
- any detriment to the child if individuals with parental responsibility cannot access this information;
- any views the child has on whether their parents should have access to information about them;

If an individual is claiming parental responsibility then they must provide a copy of the necessary evidence such as parental responsibility order or birth certificate.

A person appointed by the courts

Where are data subject is incapable of managing their affairs someone appointed to act on their behalf by a court of law may submitted a subject access request. Proof of the court order must be given.

Solicitors acting on behalf of the data subject or insurance company

Where a solicitor, lawyer or other legal professional requests access on behalf of the data subject, the signed consent of that subject must be obtained and evidenced. The request must be dealt with in the same way as if it had come direct from the data subject.

Other agencies

In some circumstances other agencies may request information. Unless there is a legal requirement for disclosure the data subjects will be informed and their written consent sought.

Written applications

Applications by fax and email will only be acceptable with an electronic signature either from the data subject themselves or from someone who has the right of access to that record and who has the data subject's written consent.

Verbal applications

Verbal applications are dealt with locally and at the discretion of the staff member who created that record specific client episode. Any information disclosed must be recorded in the patient health record.

A verbal application is not a subject access request under the act. If the data subject raises concerns regarding any discrepancies about the information disclosed, which cannot be resolved by the staff member who created the record, then a formal application must be made in writing.

Determine the validity of the applications

Applicants must provide proof of identity (driving license, passport or birth certificate) and proof of address (utility bill or bank statement) in accordance with this policy.

Administration fees

Applications can be divided into two groups.

1. **applications from solicitors or insurance companies** on the behalf of data subjects;
2. **applications that are manifestly unfounded or excessive**
   in any case the fee to be charged will be £250 which will be quoted and must be accepted and paid before any data is disclosed.

No fee is payable to view a record where at least part of that record was made or added to within 30 days or receipt of a subject access request all 60 days as required.

Exemptions

There are a considerable number of exemptions from the right of subject access including:

- data relating to the physical, mental or health condition of the data subject to the extent to which the application would be likely to cause serious harm to the physical, mental or health condition of the data subject or other persons.
- data processed for any crime and taxation purposes where the provision of this information would likely to prejudice any of the crime and taxation purposes;
- data processed for the purposes of national security;
- data processed for the purposes of research, historic record or statistical purposes that will not cause distress to any data subject or is anonymised;
- the health record of a deceased person where the data subject's express wish not to disclose is recorded or the information is not relevant to any claim arising from the deceased person's death.
- where the data controller cannot comply with a request without disclosing information about another individual who can be identified from the information, then he is not obliged to comply with the request unless:

a. the other individual has consented to the disclosure of the information to that person making the request or
b. it is reasonable in all circumstances to comply with the request without the consent of the other individual.

Timetable for access

The requested information will whenever possible, be provide to the applicant within 30 days. However, where a fee is to be charged or the applicant has provided insufficient information to identify themselves sufficiently, the 30 day clock will not begin to run until the fee is paid or the relevant information is supplied. If compliance is not possible within this period the applicant must be advised accordingly within in the 30 day period.

Providing information

When gathering the information necessary to provide the data subject with all relevant information the following points will be considered:

- check for and remove any third-party information or obtain necessary consent;
- with relevant health professionals, decide if disclosure will result in serious physical or mental harm to the data subject or others;
- method of delivery will be agreed with the applicant, for example a meeting or by post. All Information will be posted to the applicant unless otherwise agreed.

Explanation of the data

The data is supplied to the applicant should be in an intelligible form and interpretation of technical terminology given along with abbreviations or illegibility of the records. If sight only rather than copy is requested, then arrangements must be made for a Director to be present to answer any questions as to the content of the record and to maintain supervision of the applicant whilst reviewing the record.

Inaccuracies in health records

Any inaccuracies in the record to be corrected at the request of the applicant will only be made in agreement with relevant healthcare professional or Director. If the healthcare professional does not agree with the request a note recording the matters alleged to be in accurate will be made on the record and a copy sent to the applicant.

Non-disclosure of information

Where access is to be denied the applicant will be informed and no explanation of the decision will be given. One of the following reasons from the non disclosure or partial disclosure will be included in the health record:

- disclosure may be seriously harmful to the data subjects health;

- access and would not be in accordance with the best interests or wishes of the data subject for the following reasons:

  a. disclosure might identify a third person whose approval must be sought in advance;
  b. in the case of child requesting access, the child is or is not capable of understanding the nature and purpose of the application;
  c. the applicant can challenge the LHA decision and obtain assistance through the Information Commissioner's office.

History and completion of requests

a record of the request, its current status and completion will be recorded and are maintained by LHA. A record of the information supplied to the applicant together with any comment will be retained.

Complaints procedure

Should a person have a query or disagreement any decision made regarding a data subject's access request, or any disagreement with the information provided, this will be managed by LHA.

Staff guidance to view personal files

- staff members should submit a written request to view their personal file to LHA directors;
- Directors will arrange for the staff member to view their own file in the presence of a Director, information will be made available within 30 days. Prior to the employee viewing and their personal file the Director must review the file and remove or redact items not necessary to the staff member.
- staff members may not remove or alter any item in the file;
- copies of items in the file will be supplied upon request within 30 days where reasonably practicable;
- LHA reserves the right to make a charge for these copies in accordance with the Data Protection Act as of January 2012 this fee is £10, the Director retains the discretion to waive this fee.

Exemptions to viewing personal files

- information that consists of a reference given or to be given in confidence by LHA maybe withheld. This does not apply two confidential references received by LHA;
- information identifying any third parties without that third party's consent;
- information held in accordance with the Criminal Records Bureau (CRB);
- disclosures that I received it within the previous six months;
- information identifying someone other than the staff member can be withheld;
- data held for the purposes of management planning;
- data about negotiations with an employee;
- documents protected by legal professional privileges including any legal advice.

Access by other parties

From time to time other staff members may have legitimate reasons for accessing personal files as these include:

- human resources staff needing to update or maintained files all needing to access the information held in order to undertake legitimate work;
- staff in direct line management of the staff member who require accurate information for management purposes such as compiling references or reviewing sickness absence patterns;
- directors need information to carry out legitimate LHA business;
- for any independent auditor;
- other bodies such as police and solicitors and in which case request will be forwarded to the director.

Annex 1
Equality Impact Analysis

- This is a new policy;
- Written by the Director;
- The Policy assessed is the Implementation of the GDPR regulations;
- We know that a requirement exists for the policy to be created and implemented;
- There has been no consultation - other similar policies have been examined;
- This policy applies to all staff, patients, clients, students and other users of LHA;
- The policy will be communicated to all staff members and main posts on web site and on documents for users to read and provide consent to, it will be read to those who prefer this;
- No one with any protected characteristics will be disadvantaged by this policy;
- Key stakeholders are the employer, employees and users;
- This policy will advance equality and opportunity;
- There are no foreseeable negative impacts of this policy;
- This policy and activity should promote strong and positive relationships;
- It is not likely this policy could be perceived as benefiting one group at the expense of any other.

Annexe 2
Plans for Communication & Dissemination

- all staff and consultants will be given this policy and asked to read and sign to say they have read and understood the policy and agree to its provisions;
- clients, patients will be informed of the existence of the policy and be given a summary and asked to sign to say the understand the policy and agree to its provisions.
- a summary of the policy will be available on the LHA web site.

Annexe 3
Checklist for Review and Approval

Date for review	Reviewed by	Approved by	Date published
October 2018	NA Franks	NA Franks	
March 2025	NA Franks	NA Franks	05 March 2025