Copies of all EFHL HR Policies can be found on the Intranet. All EFHL Staff are subject to EFHL HR Policies. EFHL HR Policies are non-contractual, are reviewed regularly and may be subject to change. All queries on the application or interpretation of this policy should be raised with the Head of Department or HR.

10.1 – Data Protection & Confidentiality

Purpose

This policy has two main purposes:

- To detail EFHL expectations regarding the handling of personal and sensitive data relating to residents and any individual with whom the home has business with.
- To explain the information EFHL holds on Staff.
- To explain how we seek to protect personal data and ensure that our employees understand the rules governing their use of the Personal Data to which they have access in the course of their work.

This policy applies to information relating to identifiable people (i.e. Personal Data and Special Categories of Personal Data as identified in Data Protection Act 2018 (UK GDPR)). Its purpose is to enable EFHL to:

- comply with the law;
- follow good practice;
- protect its Staff;
- protect itself.

Definitions of capitalised terms can be found in Annex 1. This policy should be read in conjunction with other EFHL Data and IT Policies.

Scope

EFHL is committed to protecting the rights and freedoms of data subjects (natural persons), the safe and secure processing of their data, in accordance with Data Protection Legislation.

Data Protection Legislation means the amended Data Protection Act 2018 (UK GDPR), the Privacy and Electronic Communications (EC Directive) Regulations 2003 and any legislation implemented in connection with the Data Protection Act 2018 (UK GDPR). This includes any replacement legislation coming into effect from time to time. Where appropriate for EU residents, good or services, it includes EU GDPR.

We hold personal data about our employees, clients, suppliers and other individuals for a variety of business purposes.

This policy applies to all EFHL employees, contractors and agents including voluntary agents (hereafter collectively referred to for brevity as ‘Staff’).

In particular, this policy requires staff to ensure that the Data Protection Lead (DPL) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

EFHL’s leadership is fully committed to ensuring continued and effective implementation of this policy and expects all EFHL employees share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action.

Issued: March 2016
Revised: Jan10, Jan11, Aug11, Sep16,Apr18, Nov 19, Jun 21, May 23
Reviewed: Jan 19,20, Jun 21, Jul 21, May 23

Copies of all EFHL HR Policies can be found on the Intranet. All EFHL Staff are subject to EFHL HR Policies. EFHL HR Policies are non-contractual, are reviewed regularly and may be subject to change. All queries on the application or interpretation of this policy should be raised with the Head of Department or HR.

10.1 – Data Protection & Confidentiality

Policy Statement

All Staff are required to read, understand and accept any policies and procedures that relate to the Personal Data that EFHL holds (e.g. this policy and any retention of data guidance).

Confidentiality often applies to a wider range of information than covered by Data Protection Legislation. For example, information that is confidential because of commercial interests, rather than personal rights. In cases where someone will be working with confidential information they will be additionally required to work within the remit of specific organisational or departmental guidelines or sign non-disclosure agreements etc. These guidelines should include mechanisms for support, reporting and management of breaches.

EFHL is a Data Controller as defined under the Data Protection Act 2018 (UK GDPR). It may also act as a Data Processor when providing services to other organisations. We must maintain our appropriate registration with the Information Commissioners Office in order to continue lawfully controlling data.

As a Data Processor, we must comply with our contractual obligations and act only on the documented instructions of the data controller. As a Data Processor, we must:

- Not use a sub-processor without written authorisation of the data controller
- Co-operate fully with the ICO or other supervisory authority
- Ensure the security of the processing
- Keep accurate records of processing activities
- Notify the controller of any personal data breaches

If you are in any doubt about how we handle data, contact the DPL for clarification.

EFHL will:

- not only comply with the law but also monitor good practice guidelines from regulatory and industry bodies and follow these where appropriate;
- respect people's rights;
- be open and honest with those whose data it holds;
- provide training and support for Individuals who handle Personal Data, so that they can act confidently and consistently;
- gain assurance that all partners with whom we work operate to the standards required by the Data Protection Act 2018 (UK GDPR) and other Data Protection Legislation.

Not causing harm to people is a priority for EFHL. This means:

- keeping information securely in the right hands;
- holding good quality, accurate information;
- not holding information for longer than necessary;

Issued: March 2016
Revised: Jan10, Jan11, Aug11, Sep16,Apr18, Nov 19, Jun 21, May 23
Reviewed: Jan 19,20, Jun 21, Jul 21, May 23

Copies of all EFHL HR Policies can be found on the Intranet. All EFHL Staff are subject to EFHL HR Policies. EFHL HR Policies are non-contractual, are reviewed regularly and may be subject to change. All queries on the application or interpretation of this policy should be raised with the Head of Department or HR.

10.1 – Data Protection & Confidentiality

- only holding information that is necessary and proportionate for the conduct of its business

EFHL designates a Data Protection Lead (DPL) to provide advice and guidance on matters related to data protection.

1. Application of Policy

Staff can find out who the current DPL is by consulting their line manager or HR. At the time of writing the DPL is the IT Director.

The purpose of this policy is to provide guidance on the data protection principles that all those acting on behalf of EFHL must adhere to when any personal data belonging to or provided by data subjects is collected, stored or transmitted.

It is therefore imperative that all those who access this policy, including employees and contractors, comply with the Data Protection Principles, summarised below.

Personal Data (information identifying a living person) should:

1) Be processed fairly, lawfully and transparently
2) Be collected and processed only for specified, explicit and legitimate purposes (purpose limitation)
3) Be adequate, relevant and limited for the purposes for which it is processed. Any data collected must be necessary and not excessive for its purpose. (data minimisation)
4) Be kept accurate and up to date. Any inaccurate data must be deleted or rectified without delay (accuracy)
5) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (storage limitation)
6) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

Accountability and transparency

We must ensure accountability and transparency in all our use of personal data. Data protection legislation obliges all employees to take a proactive approach to data protection.

Lawful basis for processing data

We must establish a lawful basis for processing data.

Issued: March 2016
Revised: Jan10, Jan11, Aug11, Sep16,Apr18, Nov 19, Jun 21, May 23
Reviewed: Jan 19,20, Jun 21, Jul 21, May 23

Copies of all EFHL HR Policies can be found on the Intranet. All EFHL Staff are subject to EFHL HR Policies. EFHL HR Policies are non-contractual, are reviewed regularly and may be subject to change. All queries on the application or interpretation of this policy should be raised with the Head of Department or HR.

10.1 – Data Protection & Confidentiality

Employees must ensure that any data they are responsible for managing or working with has a written lawful basis approved by the DPL.

At least one of the following conditions must apply whenever we process personal data:

1. **Consent**
   We hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose.
2. **Contract**
   Processing is necessary to fulfil or prepare a contract for the individual.
3. **Legal obligation**
   Processing is necessary to meet a legal obligation (excluding a contract).
4. **Vital interests**
   Processing is necessary to protect a person's life or in a medical situation.
5. **Public function**
   Processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law.
6. **Legitimate interest**
   Processing is necessary for the business/organisation's legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest.

Deciding which condition to rely on

When making an assessment of the lawful basis, you must first establish that the processing is necessary. This means the processing must be a targeted, appropriate way of achieving the stated purpose. You cannot rely on a lawful basis if you can reasonably achieve the same purpose by some other means.

EFHL's commitment to the first Principle requires us to document this process and show that we have considered which lawful basis best applies to each processing purpose, and fully justify these decisions.

We must also ensure that individuals whose data is being processed by us are informed of the lawful basis for processing their data, as well as the intended purpose. This occurs via a privacy notice, which should be read in conjunction with this policy. This applies whether we have collected the data directly from the individual, or from another source.

EFHL will ensure that all staff are up to date with the Data Protection Act 2018 (UK GDPR) training and comply with its principles of good information handling (see below). These principles must also be considered in the design and implementation of all processes and procedures involving Personal Data.

Copies of all EFHL HR Policies can be found on the Intranet. All EFHL Staff are subject to EFHL HR Policies. EFHL HR Policies are non-contractual, are reviewed regularly and may be subject to change. All queries on the application or interpretation of this policy should be raised with the Head of Department or HR.

10.1 – Data Protection & Confidentiality

Security

In order to ensure that EFHL is complying with the Data Protection Act 2018 (UK GDPR), all Staff who have responsibility for, or hold, Personal Data, either on a computer system or any other relevant system (including paper) are responsible for its secure processing and storage. In effect, this means that physical data shall be locked away when not in use and that suitable security systems are in place for electronic storage.

Practical examples of good information handling might include:

- Ensuring that all systems are accurate, up to date and processed in accordance with the Data Protection Act 2018 (UK GDPR);
- Only disclosing Personal Data where authorised, and then only in accordance with the Data Protection Act 2018 (UK GDPR) on a 'need and right to know' basis;
- treating all Personal Data with care;
- Checking the identities of people before disclosing information by telephone, e-mail or letter;
- Ensuring that security measures are adequate (locks, passwords etc);
- Not leaving computer screens unattended when 'logged in';
- Keeping a 'clear desk' policy
- Data stored on a computer should be protected by strong passwords that are changed regularly.
- Data stored on CDs or memory sticks must be encrypted or password protected and locked away securely when they are not being used. External storage devices may only be used with the express permission of the IT Department, who will ensure the device is encrypted and only used for a specific activity if there is a systems issue.
- The DPL must approve any cloud used to store data
- Systems containing personal data must be kept in a secure location, away from general office access.
- Data should be regularly backed up in line with the company's backup procedures.
- Data must never be saved directly to mobile devices such as laptops, tablets or smartphones. This includes information in emails.
- Personal or special categories of data should not be forwarded to personal or other unauthorised email addresses.
- Public Wi-Fi ('Wi-Fi hotspots') must not be used to access personal or special categories of data.
- All servers containing sensitive data must be approved and protected by security software.
- All possible technical measures must be put in place to keep data secure.
- Disposing of waste printed matter as confidential waste.
- Removal/redaction of non-essential Personal Data when storing or sharing information.
- When appropriate, ensuring Personal Data is pseudonymised (eg key-coded). It is important to consider how difficult it is to attribute the pseudonym to an individual.
-

Issued: March 2016
Revised: Jan10, Jan11, Aug11, Sep16,Apr18, Nov 19, Jun 21, May 23
Reviewed: Jan 19,20, Jun 21, Jul 21, May 23

Copies of all EFHL HR Policies can be found on the Intranet. All EFHL Staff are subject to EFHL HR Policies. EFHL HR Policies are non-contractual, are reviewed regularly and may be subject to change. All queries on the application or interpretation of this policy should be raised with the Head of Department or HR.

10.1 – Data Protection & Confidentiality

Special Categories of Personal Data
The Data Protection Act 2018 (UK GDPR) equivalent of the original DPA's Sensitive Personal Data is 'Special Categories of Personal Data'. It includes information about an individual's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics for ID, health, sex life and orientation. Unlike the previous legislation, it does not include data relating to criminal offenses and convictions, because these are addressed by specific safeguards elsewhere in the Data Protection Act 2018 (UK GDPR).

Like Personal Data, you must still have a lawful basis for processing Special Categories of Personal Data, but because it is more sensitive it has more protection. To process it you need to satisfy a special condition (specified in Article 9 of the Data Protection Act 2018 (UK GDPR)). The conditions of Article 9 are listed in Annex 2.

Children's Personal Data
The Data Protection Act 2018 (UK GDPR) recognises that children need particular protection when their personal data is collected and processed because they may be less aware of the risks involved. It would be unusual for FHL to process data related to children and consent from a parent/guardian would be expected; we would not normally process children's data directly from a minor. Since the issues surrounding the protection of children and their personal data is complex, the DPL should always be consulted should there be new processes or changes to existing processes that involve children's data, Staff should also refer to 'New and Changed Processes, Projects and Initiatives' below.

Criminal record checks
Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject. We cannot keep a comprehensive register of criminal offence data. All data relating to criminal offences is considered to be a special category of personal data and must be treated as such. You must have approval from the DPL prior to carrying out a criminal record check.

Concerns or Failure to Comply
If a member of staff believes that there has been a failure to comply with the Data Protection Act 2018 (UK GDPR), or is concerned about a practice that may potentially result in contravention of the Act, they must seek the guidance of their line manager (who in turn must discuss with the DPL). Relatives, volunteers, contractors and similar should seek guidance from their main EFHL contact (who in turn must discuss with the DPL). Members of staff should not contact external agencies such as the ICO directly; this should be done by the DPL to ensure a coordinated overview of any situation is presented.

No member of Staff should fear raising concerns – see the EFHL HR Policy 9.3 Whistleblowing (Public Interest Reporting) Policy.

Individuals rights
The Data Protection Act 2018 (UK GDPR) provides the following rights for individuals (i.e. people who engage with EFHL including Staff):

1. The right to be informed
2. The right of access

Issued: March 2016
Revised: Jan10, Jan11, Aug11, Sep16,Apr18, Nov 19, Jun 21, May 23
Reviewed: Jan 19,20, Jun 21, Jul 21, May 23

Copies of all EFHL HR Policies can be found on the Intranet. All EFHL Staff are subject to EFHL HR Policies. EFHL HR Policies are non-contractual, are reviewed regularly and may be subject to change. All queries on the application or interpretation of this policy should be raised with the Head of Department or HR.

10.1 – Data Protection & Confidentiality

3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

The Office of Information Commissioner website (www.ico.org.uk) should be used as the primary source for guidance on these rights. However, this guidance provides an overview:

1. The right to be informed
This covers EFHL' obligation to provide 'fair processing information', through a privacy notice which is provided. It emphasises the need for transparency over how EFHL use Personal Data.

Any member of Staff creating systems or processes should insure that Data Protection Legislation is an explicit part of the project plan and that the appropriate member of Executive Team is informed. It is then Executive Team's responsibility to ensure the system is reviewed by the DPL (they may designate this).

2. The right of access
Under Data Protection Act 2018 (UK GDPR), individuals have the right to obtain confirmation that their data is being processed; access to their Personal Data; and other supplementary information which largely corresponds to the information that is provided in the EFHL privacy notice.

EFHL requires that all Subject Access Requests must be passed to the DPL through HR or the Executive Team without undue delay. EFHL has a duty to ensure the request is complied with within one month of the request being received.
Normally the request must be fulfilled free of charge. A fee based on the administrative cost can only be charged in cases where a request is manifestly unfounded or excessive (particularly if it is repetitive).

3. The right to rectification
Individuals are entitled to have Personal Data rectified if it is inaccurate or incomplete. Requests for rectification must be passed to the DPL through HR or the Executive Team without undue delay.

If EFHL has disclosed the Personal Data in question to others, each recipient must be contacted and informed of the rectification - unless this proves impossible or involves disproportionate effort. If asked to, EFHL must also inform the individuals about these recipients.

EFHL must respond to the request within one month (this can be extended by two months where the request for rectification is complex). Where EFHL is not acting in response to a request for rectification, this must be explained, along with the individual's right to complain to the supervisory authority and to a judicial remedy.

Copies of all EFHL HR Policies can be found on the Intranet. All EFHL Staff are subject to EFHL HR Policies. EFHL HR Policies are non-contractual, are reviewed regularly and may be subject to change. All queries on the application or interpretation of this policy should be raised with the Head of Department or HR.

10.1 – Data Protection & Confidentiality

4. The right to erasure
Also known as the 'right to be forgotten', this is complex and not an absolute right. In general terms, Personal Data must be erased when no longer necessary; if consent is withdrawn or if the processing is objected to or was unlawful. However, there are some specific circumstances where the right to erasure does not apply.

Requests for erasure must be passed to the DPL through HR or the Executive Team without undue delay. If, as a member of staff, you receive a request for erasure you must inform your line manager or any member of HR without undue delay.

6. The right to restrict processing
Such a request would mean that EFHL is allowed to store the data, but not further process it. After such a request EFHL would be able to retain just enough information to ensure the restriction is respected in future.

Requests for erasure must be passed to the DPL through HR or the Executive Team without undue delay. If, as a member of Staff, you receive a request to restrict processing you must inform your line manager or any member of HR without undue delay.

7. The right to object
Individuals have the right to object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (again including profiling) and processing for purposes of scientific/historical research and statistics.

The most likely of these reasons to affect EFHL is that of direct marketing, though research and statistics is also possible. EFHL must inform individuals of their right to object "at the point of first communication" and in its privacy notice. There must be a way to object online.

As a Staff member, you must inform your line manager of any such request, and whether you are able to comply. Managers should ensure that the request is complied with or referred to HR without undue delay.

8. Rights in relation to automated decision making and profiling
Any member of Staff creating systems or processes that involves automated decision making or profiling should insure that Data Protection Legislation in general, and in particular the Data Protection Act 2018 (UK GDPR) is an explicit part of the project plan and that the appropriate member of the Executive Team is informed. It is then the Executive Team's responsibility to ensure the system is reviewed by the DPL (they may designate this).

Third Party Requests
Request for information from outside bodies (such as the police, HMRC, journalists) should be immediately passed to the appropriate Director/Head of Department, or in their absence any member of SMT. Typically they will refer this to the DPL unless the request is straightforward.

The request will be considered in accordance with the strict wording of the Data Protection Act 2018 (UK GDPR), or if appropriate EU GDPR. In the case of the police and HMRC this will

Copies of all EFHL HR Policies can be found on the Intranet. All EFHL Staff are subject to EFHL HR Policies. EFHL HR Policies are non-contractual, are reviewed regularly and may be subject to change. All queries on the application or interpretation of this policy should be raised with the Head of Department or HR.

10.1 – Data Protection & Confidentiality

typically be in the form of a written request explaining the reason for the request. In the case of local authorities or government departments, the legal authority must be established. The DPL and/or the Information Commissioner's Office may be consulted.

Safeguarding and the Data Protection Act 2018 (UK GDPR)
In certain safeguarding matters, it is permissible to process special category data without consent where: it is justified; is in the public interest and necessary to safeguard an individual. In such matters staff must consult the General Manager or HR immediately.

Training
Staff training in Data Protection is mandatory. It is each Staff member's responsibility to ensure they are up to date with policy using the materials provided and should ensure they review relevant training material and/or training sessions at least annually.

New and Changed Processes, Projects and Initiatives
It is important that the Data Protection Act 2018 (UK GDPR) is inherent in the design of any new processes, projects and initiatives and is also formally considered as part of any changes to existing processes, projects and initiatives. Those managing the new or existing process, project or initiative must document the personal data implications and data protection risks ensure they are assessed and approved by the DPL. This assessment will include both the handling and storage or personal data. This risk assessment is called a Data Protection Impact Assessment (DPIA). Also see National Data Opt Out below.

It is recognised that for changes a degree of pragmatism is required – for example the DPL would not need to be consulted if a column title was changed from 'Surname' to 'Last-name'. If in doubt, guidance from a line manager should be sought.

The Freedom of Information Act 2000

EFHL is not bound by the Freedom of Information Act. It does however uphold the spirit of the Act in its broadest sense and believes that people have a right to know about its activities unless there is a compelling reason otherwise (such as Safeguarding, vexatious requests, Data Protection Act 2018 (UK GDPR) compliance, business confidentiality/competition etc.).

Information held about Staff

The Data Protection Act 2018 (UK GDPR) regulates the way in which certain information about Staff is held and used. This section of the policy provides details about the type of information that EFHL keeps about Staff and the purposes for which it keeps this information.

Throughout the employment/relationship with EFHL, and for as long a period as is necessary following the termination of employment/relationship, EFHL will need to keep information for purposes connected with a member of Staff's employment/relationship, including recruitment and termination information. These records may include:

- information gathered about a Staff member and any references obtained during recruitment or engagement.
- details of terms of employment/engagement.

Copies of all EFHL HR Policies can be found on the Intranet. All EFHL Staff are subject to EFHL HR Policies. EFHL HR Policies are non-contractual, are reviewed regularly and may be subject to change. All queries on the application or interpretation of this policy should be raised with the Head of Department or HR.

10.1 – Data Protection & Confidentiality

- payroll, tax and national insurance information.
- performance information.
- details of grade and job duties.
- health records.
- absence records, including holiday records.
- details of any disciplinary investigations and proceedings.
- training records.
- contact names and addresses.
- correspondence with EFHL and other information provided to EFHL.

EFHL believes these records are consistent with our employment/relationship and the principles of the Data Protection Act 2018 (UK GDPR). The information held will be for management and administrative use only but, from time to time, we may need to disclose certain information we hold about Staff to relevant third parties e.g. where legally obliged to do so by HMRC, or requested to do so by a Staff member for the purposes of giving a reference. We may also transfer information to another group or organisation, solely for purposes connected with a member of Staff's career or the management of EFHL business.

It should also be noted that EFHL might hold information about Staff for which disclosure to another party will be made only when strictly necessary for the purposes set out below:

- a member of Staff's health, for the purposes of compliance with our health and safety and occupational health obligations.
- for the purposes of human resources management and administration e.g. to consider how a member of Staff's health affects their ability to do their job and, if the Staff member is disabled, whether they require any reasonable adjustment to be made to assist them in their role.
- the administration of payroll, insurance, pension, sick pay and any other related benefits in force from time to time.
- in connection with convictions to enable us to assess an individual's suitability for employment/engagement.

Staff Right of Access to Information
In accordance with the Data Protection Act 2018 (UK GDPR) all Staff have the right to access any Personal Data that is kept about them either on computer or in certain files. Any member of Staff who wishes to exercise this right should make this request in writing to the HR Department. EFHL will aim to comply with any request for access to Personal Data without delay and within the timeframe required by the Data Protection Act 2018 (UK GDPR). Please see the Data Subject Access Request Policy.

EFHL would not normally make a charge for providing access to Personal Data. However, it reserves the right to charge a reasonable fee when a request is manifestly unfounded or excessive, particularly if it is repetitive.

EFHL requires all Staff to comply with the Data Protection Act 2018 (UK GDPR) in relation to the information about other Staff. Staff in a position that deals with personal information about

Copies of all EFHL HR Policies can be found on the Intranet. All EFHL Staff are subject to EFHL HR Policies. EFHL HR Policies are non-contractual, are reviewed regularly and may be subject to change. All queries on the application or interpretation of this policy should be raised with the Head of Department or HR.

10.1 – Data Protection & Confidentiality

other Staff must treat this information in strict confidence. Any deliberate or careless breach of this Policy will be regarded as serious misconduct and will be dealt with in accordance with EFHL Disciplinary Policy and Procedures.

Individuals Handling Personal Data

All Staff have a duty, both during their employment/relationship with EFHL and after their employment/relationship has ended, not to reveal any confidential information unless required to do so by a court of law.

EFHL Contracts of Employment contain a confidentiality clause, which details Staff members' responsibilities.

If Staff are asked for information which they think is or may be confidential, they must consider the following:

- All media (press, television, etc) enquiries must be referred in the first instance to the General Manager and the Executive team at headquarters. It is important that no interviews or statements should be given without prior clearance.
- All enquiries from the police should be referred to the HR Department for Staff related issues or a member of SMT (as appropriate).
- Staff required to give evidence in a court of law should inform the appropriate Director/Head of Department or HR without delay.

Staff requiring access to another Staff member's email or personal files (e.g. after the Staff member has left the organisation) must refer to IT and/or HR. Any access permitted will be supervised by IT and/or HR to help maintain confidentiality.

If in doubt staff should consult their line manager and/or HR. They in turn may consult the DPL.

Data Breaches

Any breach of this policy or of data protection laws must be reported as soon as practically possible. This means as soon as you have become aware of a breach. EFHL has a legal obligation to report any data breaches to the ICO within 72 hours.

- All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:
- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the ICO of any compliance failures that are material either in their own right or as part of a pattern of failures

Any member of staff who fails to notify of a breach, or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.

Please refer to our Data Breach Policy for our reporting procedure.

Copies of all EFHL HR Policies can be found on the Intranet. All EFHL Staff are subject to EFHL HR Policies. EFHL HR Policies are non-contractual, are reviewed regularly and may be subject to change. All queries on the application or interpretation of this policy should be raised with the Head of Department or HR.

10.1 – Data Protection & Confidentiality

Using third party controllers and processors

As a data controller, we must have written contracts in place with any third-party data processors that we use. The contract must contain specific clauses which set out our and their liabilities, obligations and responsibilities.

As a data controller, we must only appoint processors who can provide sufficient guarantees under Data Protection Act 2018 (UK GDPR) that the rights of data subjects will be respected and protected.

Copies of all EFHL HR Policies can be found on the Intranet. All EFHL Staff are subject to EFHL HR Policies. EFHL HR Policies are non-contractual, are reviewed regularly and may be subject to change. All queries on the application or interpretation of this policy should be raised with the Head of Department or HR.

10.1 – Data Protection & Confidentiality

Contracts

Our contracts must comply with the Data Protection Act 2018 (UK GDPR) contractual clauses and where applicable, any other requirements set out by the ICO. Our contracts with data processors must set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller.

At a minimum, our contracts must include terms that specify:

- Acting only on written instructions
- Those involved in processing the data are subject to a duty of confidence
- Appropriate measures will be taken to ensure the security of the processing
- Sub-processors will only be engaged with the prior consent of the controller and under a written contract
- The controller will assist the processor in dealing with subject access requests and allowing data subjects to exercise their rights under the Data Protection Act 2018 (UK GDPR)
- The processor will assist the controller in meeting its Data Protection Act 2018 (UK GDPR) obligations in relation to the security of processing, notification of data breaches and implementation of Data Protection Impact Assessments
- Delete or return all personal data at the end of the contract
- Submit to regular audits and inspections, and provide whatever information necessary for the controller and processor to meet their legal obligations.
- Nothing will be done by either the controller or processor to infringe on the Data Protection Act 2018 (UK GDPR).

Data retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines (please see the Data Retention Policy). A copy of our Retention schedule can be obtained on request from the DPL.

Transferring data internationally

There are restrictions on international transfers of personal data. You must not transfer personal data abroad, or anywhere else outside of normal rules and procedures without express permission from the DPL.

National Data Opt Out

All health and social care CQC-registered organisations in England must be compliant with the national data opt out by 31 March 2021. The national data opt-out gives everyone the ability to stop health and social care organisations from sharing their confidential information

Copies of all EFHL HR Policies can be found on the Intranet. All EFHL Staff are subject to EFHL HR Policies. EFHL HR Policies are non-contractual, are reviewed regularly and may be subject to change. All queries on the application or interpretation of this policy should be raised with the Head of Department or HR.

10.1 – Data Protection & Confidentiality

for research and planning purposes, with some exceptions such as where there is a legal mandate/direction or an overriding public interest for example to help manage the covid-19 pandemic.

Routinely, EFHL would not share personal information for any reason other than direct management of care. However, any new or changed process, project or initiative must be compliant with the National Data Opt Out.

Copies of all EFHL HR Policies can be found on the Intranet. All EFHL Staff are subject to EFHL HR Policies. EFHL HR Policies are non-contractual, are reviewed regularly and may be subject to change. All queries on the application or interpretation of this policy should be raised with the Head of Department or HR.

10.1 – Data Protection & Confidentiality

Annex 1 - Definitions

Data Controller	A person or organisation who determines the purposes for which and the manner in which any Personal Data are, or are to be, processed.
Data Protection Act 2018 (DPA)	The UK legislation that provides a framework for responsible behaviour by those using personal information. It was amended as EU GDPR law was brought into UK law (UK GDPR). The amended form took effect on January 31, 2020.
Data Protection Impact Assessment	A Data Protection Impact Assessment (DPIA) describes a process designed to identify risks arising out of the processing of personal data and to minimise these risks as far and as early as possible. DPIAs are important tools for negating risk, and for demonstrating compliance with the GDPR.
Data Protection Lead (DPL)	The person(s) responsible for ensuring that the organisation follows its data protection policy and complies with the Data Protection Act 1998
Data Processor	Means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.
Data Subject	Means an individual who is the subject of Personal Data.
GDPR	The General Data Protection Regulations as ratified by the European Union in 2016 and enforceable from 25 May 2018. Refered to as EU GDPR in this document. The GDPR was brought into UK law on January 31, 2020 (UK GDPR).
Information Commissioner's Office (ICO)	The UK Information Commissioner responsible for implementing and overseeing the GDPR.
Personal Data	Personal Data means data which relate to a living individual who can be identified – (a) from that data, or (b) from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.
Right of Subject Access	The right of an individual who makes a written request to be told whether any Personal Data is being processed; given a description of the Personal Data, the reasons it is being processed, and whether it will be given to any other organisations or people; given a copy of the information comprising the data; and given details of the source of the data (where available) and the reasoning behind any automated decisions, such as a computer-generated decision. Responses to Subject Access requests must be prompt and within one month.
Sensitive Personal Data	A DPA definition that means data about racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health, sexual life, criminal record, criminal proceedings relating to a Data Subject's offences
SMT	Senior Management Team: the executive team of the Company.

Issued: March 2016
Revised: Jan10, Jan11, Aug11, Sep16,Apr18, Nov 19, Jun 21, May 23
Reviewed: Jan 19,20, Jun 21, Jul 21, May 23

Copies of all EFHL HR Policies can be found on the Intranet. All EFHL Staff are subject to EFHL HR Policies. EFHL HR Policies are non-contractual, are reviewed regularly and may be subject to change. All queries on the application or interpretation of this policy should be raised with the Head of Department or HR.

10.1 – Data Protection & Confidentiality

Special Categories of Personal Data	A GDPR category of data which is more sensitive that other Personal Data and specifically includes race, ethnic origin, politics, religion, trade union membership, genetics, biometrics for ID, health, sex life and orientation. Unlike the DPA Sensitive Personal Data it does not include data relating to criminal offenses and convictions, because these are addressed by specific safeguards elsewhere in the GDPR).
Staff member or member of Staff	A collective term used for EFHL' trustees, employees, contractors and agents including voluntary agents.
UK GDPR	See GDPR.

Copies of all EFHL HR Policies can be found on the Intranet. All EFHL Staff are subject to EFHL HR Policies. EFHL HR Policies are non-contractual, are reviewed regularly and may be subject to change. All queries on the application or interpretation of this policy should be raised with the Head of Department or HR.

10.1 – Data Protection & Confidentiality

Annex 2 - The rules for processing special category data

The conditions are listed in Article 9(2) of the Data Protection Act 2018 (UK GDPR) are detailed at:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/

If Staff have any queries about this policy or Data Protection in general, they should contact their Head of Department or HR or the DPL.