1. Purpose & Scope

All employees are expected to be familiar with key UK Data Protection Act 2018 & EU General Data Protection Regulations (GDPR) rules and terminology – as 'data processors' & 'data handlers'. This Data Protection Policy is concerned primarily with client and third-party data – which we all have a duty to protect.

2. Definitions

2.1 Personal information/data

Personal information/data relates to a living individual who can be identified from the information (or from that information and any other information in the possession of Document Genetics). This includes both factual information and opinion as expressed by a third party.

2.2 Sensitive personal information/data

Sensitive personal information/data attracts additional protection in law and is considered by the Information Commissioner's Office (ICO) to be any data that could lead to the identification of a person and is overtly personal in nature. Example of this would include personal data consisting of information such as:

- the racial or ethnic origin;
- political opinions;
- religious beliefs or other beliefs of a similar nature;
- membership of a trade union;
- physical or mental health or condition;
- sex life/ sexual orientation;
- commission or alleged commission of any offence;
- any proceeding for any offence committed or alleged to have been committed or disposal of such proceedings or the sentence of court in such proceedings;
- details of bank account, national insurance number, any ID details such as passport or driving licence, etc.

2.3 A data record can be:

In computerised and/or manual form and may include such documentation as:

- hand written notes;
- letters to and from Document Genetics;
- electronic records;
- printouts;
- photographs;
- videos and tape recordings.

2.4 Data Subject means:

An individual who is the subject of personal data.

2.5 Data Controller means:

A person or entity who has authority to decide how personal data is to be processed or determines the purposes and manner in which any personal data is used, or will be used.

2.6 Data Processor

Data processor, in relation to personal data, means any party that processes (obtaining, recording, adapting or holding) the data on behalf of the data controller.

2.7 Data Handler of Data Extractor is:

Any party who acts as a data processor and is given access to and transfers, stores, or destroys 'data'.

3. Document Genetcis' Commitment to Client/Third Party Data

In the interest of protecting our clients' and any third-party data, Document Genetics undertakes to ensure that we:

- assign the Directors as Data Protection Officers;
- instruct all employees and contractors who manage and handle personal data so that they understand their safeguarding duties and obligations;
- regularly assess and evaluate our methods of handling personal data;
- obtain personal data only for specified and lawful purposes;
- do not keep personal data for longer than is necessary;
- process personal data in accordance with the rights of data subjects under the General Data Protection Regulation 2018;
- take measures to prevent unauthorised or unlawful processing of personal data and the accidental loss or destruction of, or damage to, personal data;
- do not transfer personal data to a country or territory outside the European Economic area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

4. Employees' Commitment to Client/Colleague/Third Party Data

In the interest of protecting our clients', colleagues' and any third party data, all employees must ensure that they:

- stop and consider whether they should be accessing or disclosing personal data before they do so;
- make sure that they have verified that the person they are passing data on to is who they say they are and that they are authorised to receive it;
- do not discuss information about clients, colleagues and third parties with unauthorised colleagues, family or friends, or Document Genetics clients;
- do not access Document Genetics business records containing personal data other than for a specific business purpose; This may also be an offence under the UK Data Protection Act 2018 and the GDPR, plus, the Company may be prosecuted by the ICO;
- avoid providing any specific detail about individuals that might lead to their identification when using information for reports or monitoring purposes unless they have given written permission for it to be used;
- do not express unsubstantiated personal opinions in file notes, e-mails or other means of communication; individuals may have a right to see the information and may exercise that right;
- give careful consideration to the use of e-mail distribution lists and the blind carbon copy (BCC) option especially when sending out e-mails to large numbers of recipients (i.e. clients, colleagues, or third parties);
- always remember to consult one of the Directors for their input before starting any projects involving the processing of personal data;
- always consider data security and the risks associated with losing personal data, before downloading/printing any personal data;
- never share their computer password or write it down; doing so could result in the unauthorised accessing of personal data and, therefore, a serious security breach;

- always lock their screen when leaving their computer – even if it's only for a few minutes – and remember to log off at the end of the day;
- never work on any Document Genetics data in a public place including use of mobile phones and laptops;
- take care not to leave documents containing personal data on the printer, photocopier or scanner (please note fax machines should not be used to transmit personal data as the ICO consider it out-dated and unsecure);
- make sure that personal data cannot be seen or accessed by unauthorised individuals either in or out of the office. If sensitive data is taken out of a building, it needs to be secure (i.e. encrypted or locked). When travelling by car papers must always be transported in the boot of the car. Papers must not be left in the car overnight; when at home in locked bag or secured cabinet;
- dispose of confidential waste and paper copies containing personal data by means of shredding;
- ensure personal data extracted for Document Genetics use is stored on encrypted memory sticks or other suitable encrypted storage. Refer to one of the Directors if encryption is required. Data uploaded to any third party web-storage must be treated with the same level of security and permission must be sought in advance of any upload;
- extract data only with approval from their line manager and be aware that the control of the data whilst extracted is the joint responsibility of the "data extractor" and their line manager.

5. Transfer of Personal Data to a Third Party

We require all employees to be aware of the following important protocols in the event that personal data is transferred to a third party.

5.1 Before personal data is transferred, a Non-Disclosure Agreement (NDA) or Data Processing Agreement (DPA) should be in place between Document Genetics and the third party. Alternatively, the third party may present terms to Document Genetics that satisfy the requirements of this clause.

5.2 The agreement between the parties, whatever its form, should clearly state the third party's obligation to treat the data in accordance with the provisions of the General Data Protection Regulation.

5.3 NDAs/DPAs are managed by the Directors and employees may assume that these are in place only when a third party is formally introduced to the Company. If you have any doubt whatsoever about the relationship that exists between Document Genetics and a third party please speak directly to one of the Directors and do not transfer any personal data to the third party until you have done so.

5.4 Please be aware that personal data transfer beyond the UK and EU is subject to special arrangements. As above, if you have any doubt whatsoever about the relationship that exists between Document Genetics and a non-UK or non-EU third party please speak directly to the one of the Directors and do not transfer any personal data to the third party until you have done so.

5.5 If you are responsible for transferring data to a third party please be aware of the following precautions:

- if data is sent via a courier the intended recipient must be advised when to expect the data;
- the recipient must confirm safe receipt as soon as the data arrives;

- data must not be transferred outside of the Company network other than to an authorised recipient, such as a client or contractor. If sent via the internet, all personally identifiable data must be either password protected and/or encrypted;
- never transfer third party personal data to your personal cloud account, memory stick, email account or similar. This may result in disciplinary action and/or enforcement action by the Information Commissioner's Office.

5.6 External Transfer of Personal and Sensitive Data

5.6.i Principle

The following guidance sets out how personal and/or sensitive information should be processed to ensure that our clients', colleagues' or any third party's data is in no way compromised. This includes the transferring, storage and disposal of information and information held on our behalf by contractors. If you have personal information that is currently stored or transferred insecurely, you must secure it immediately.

5.6.ii Transferring Personal and/or Sensitive Data by Email

Please observe the following essential protocols for personal and/or sensitive data transfer via email:

- sensitive information (see 'definitions' above) relating to a single individual can be sent via email attachment to the subject of the information if they have requested it to be sent by email or with their agreement and it is encrypted. The exception to this is when the individual has stated that they want to receive the information without encryption. A record must be kept of this request;
- documents containing sensitive personal information cannot be sent to third parties without encryption and should not be contained within the body of an email but attached as an encrypted document;
- care should be taken when addressing email messages to ensure a correct, current address is used and the email is only copied to those with a legitimate business interest;
- if information is transmitted and not received by the intended recipient, check that contact details and email address are correct for the receiving party before re-sending;
- consider the impact on individuals of the data being lost or misdirected. Where information is provided in bulk or where the information is of a sensitive nature make an assessment on the protection to be applied. If in doubt, send information in an encrypted attachment to the email;
- avoid putting sensitive personal information about more than one person in an email as this will lead to difficulties in maintaining accurate and relevant individual client or staff records;
- when transferring data be aware of who has permission to view your emails or who might be able to view your recipient's inbox;
- where email and personal data are stored or accessed on any mobile device, such device must be protected with a password/PIN/finger print or other secure login means.

5.7 Dealing with a Data Breach

5.7.i If a data breach is suspected staff should immediately notify one of the Directors.

5.7.ii Following notification Document Genetics will record the breach on the Information Security Incident Report form.

5.8 Breach of the Document Genetics Data Protection Policy

In the event that an employee fails to comply with this Policy, the matter may be considered as misconduct and dealt with in accordance with Document Genetics' Disciplinary Policy and procedure.

6. Removable Media

6.1 In line with our commitment to safeguard not only our own but our clients' and other third parties' confidential information, we require all employees to conform with our policy on removable media. For clarity, 'removable media' will include – amongst other things - CDs, DVDs, optical disks, external hard drives, USB memory sticks (pen drives or flash drives), media card readers, Smart cards, SIM cards, and digital cameras.

Misuse of removable media can result in:

- disclosure of protected and restricted information as a consequence of loss or theft;
- contamination of Company networks or equipment through the introduction of viruses through the transfer of data from one form of IT equipment to another;
- potential legal action against the Company or individuals as a result of information loss or misuse;
- significant reputational damage for Document Genetics.

6.2 The only equipment and media that should be used to connect to Company equipment or the network is equipment and media that has been purchased by the Company and approved by one of the Directors.

6.3 Data stored on removal media must be backed up/copied on the source system or a networked computer.

6.4 All removable media devices must be encrypted/secured.

6.5 Any suspected breaches of information security (loss/damage/theft) must be immediately reported to one of the Directors.

6.6 No third party may receive data or extract information from the Company's network, information stores or IT equipment without the explicit agreement of one of the Directors. Furthermore, the third party will be required to sign a Non-Disclosure and Confidentiality Agreement and must be made fully aware of our Data Protection Policy.

6.7 Damaged or obsolete removable media must be securely disposed of or erased to avoid data leakage.