Data Protection Policy

Name of organisation: Talking Lab

1. Introduction

The Data Protection Act (DPA) 2018 sets out the framework for data protection law in the UK. It was amended on 01 January 2021 by regulations under the European Union (Withdrawal) Act 2018, to reflect the UK's status outside the EU. It sits alongside and supplements the UK GDPR.

The UK GDPR is the UK General Data Protection Regulation. It is a UK law which came into effect on 01 January 2021. It sets out the key principles, rights and obligations for most processing of personal data in the UK, except for law enforcement and intelligence agencies. It is based on the EU GDPR (General Data Protection Regulation (EU) 2016/679) which applied in the UK before that date.

Talking Lab needs to comply with the DPA, the UK GDPR and with the EU GDPR in the event of offering goods or services to individuals in Europe.

The Act and the UK GDPR apply to personal data and special categories of personal data which are subject to more stringent conditions for processing.

Talking Lab must take adequate measures to protect personal data, ensure it is transparent in its use and that it is accountable for demonstrating its compliance with the legislation. It must also comply with the newly enhanced rights of individuals which give them more control over their information.

2. Purpose

The purpose of this policy is to ensure all staff (paid or unpaid) who have access to any personal data are fully aware of and abide by their duties and responsibilities under the Act and the UK GDPR.

3. Scope

This policy applies to any records held by or on behalf of Talking Lab or those that the Talking Lab holds in its capacity as a Data Processor, which relate to an identified or identifiable natural person, in any format. This includes - but is not limited to - electronic and paper records, images including photographs, video clips and sound recordings.

4. Statement of Policy

In order to operate efficiently, Talking Lab has to collect and use information about the people it serves and with whom it works. These may include members of the public, clients and customers, current, past and prospective employees. It may be necessary or sometimes a statutory requirement to share information with external parties. Whatever

the purpose and however it is collected, recorded or used, personal information must be handled appropriately and lawfully at all times.

5. Definitions

5.1 Personal Data

Personal data is defined as any information relating to an identified or identifiable living individual. That individual must be identified either directly or indirectly from one or more identifiers or from factors specific to the individual.

5.2 Special Category Data

Special Category data is defined as personal data consisting of information as to:

- race;
- ethnic origin;
- politics;
- religion;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.
- Unless otherwise specified, reference to “personal data” includes special category data throughout this policy.

5.3 Processing

Processing covers a wide range of operations performed on personal data, including by manual or automated means. It includes the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data.

5.4 Data Controller

A Data Controller is the entity that determines the purposes, conditions and means of the processing of personal data.

5.5 Data Processor

A Data Processor is the entity that processes data on behalf of and under the instruction of the Data Controller.

5.6 Record of Processing Activity

A Record of Processing Activity (ROPA) logs the details and purposes of any

processing of personal data. It includes details of processing carried out in its capacity as Data Processor for another organisation. The Council's Information Asset Register constitutes the ROPA.

6. **General Responsibilities**
   - Talking Lab, as a corporate body, is named as the Data Controller under the Act.
   - All Talking Lab staff are responsible for compliance with the Act, the UK GDPR, this Policy and associated documents.
   - The Chief Executive is the Director, who has overall responsibility for compliance

7. **The Principles**

The Act stipulates that anyone processing personal data must comply with six legally enforceable Principles of good practice. Talking Lab will have policies and processes in place to ensure its compliance with the principles as follows:-

Principle 1 - The processing of personal data is lawful, fair and transparent.

In response, Talking Lab will ensure:

- Personal data is only processed where there is a legal basis for doing so and in addition, where special category data is processed, a condition for processing is identified (see appendix 1)
- Explicit consent is obtained and recorded when no other legal basis exists
- Publication of privacy information (details of the personal information to be collected, its purpose, who it is shared with etc.) is clear, accessible and carried out in a timely manner
- Personal data is shared appropriately and barriers to lawful sharing are overcome. A suitable agreement is in place, regularly reviewed and monitored where personal data is to be shared with another Data Controller
- The rights of people about whom personal data is held can be fully exercised under the Act and within the statutory timescale, including the right to be informed, to rectification, erasure, restricting of processing, data portability and to object in certain circumstances

Principle 2 - The purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and that personal data so collected must not be processed in a manner that is incompatible with the purpose for which it is collected.

In response, Talking Lab will ensure:

- All staff are aware that personal data must only be used for the specified purpose or closely related purposes

- A lawful basis is identified and a contract or written agreement detailing the terms and conditions for processing is in place and regularly monitored, where carried out by a Data Processor
- A lawful basis is identified and a suitable agreement is in place, regularly reviewed and monitored where personal data is to be shared with another Data Controller

Principle 3 - Personal data is adequate, relevant and not excessive in relation to the purpose for which it is processed.

In response, Talking Lab will ensure:

- All personnel receive appropriate guidance in creating records

Principle 4 - Personal data undergoing processing is accurate and, where necessary, kept up to date.

In response, Talking Lab will ensure:

- Business processes are in place to ensure records are regularly reviewed and audited for quality and accuracy

Principle 5 - Personal data is kept for no longer than is necessary for the purpose for which it is processed.

In response, Talking Lab will ensure:-

- Records are appropriately managed and destroyed.
- There is no statutory guidance which states how long information is required to be stored for. Therefore, Talking Lab follows the Retention Periods Guidance from the Information and Records Management Society (IRMS).
- Data will be stored until a child's 25th birthday or 8 years post the last point of contact, whichever is furthest date into the future.
- After this point, all electronic data will be destroyed and deleted.
- Talking Lab does not store any paper documents. Any paper documents containing personal data are redacted, then scanned onto the electronic database and shredded.

Principle 6 - Personal data is processed in a manner that includes taking appropriate security measures as regards risks that arise from processing personal data.

In response, Talking Lab will ensure:-

All personnel processing personal data are appropriately trained to do so and have regular refresher training;

- All personnel processing personal data are appropriately supervised;
- Anyone wanting advice or guidance about processing personal data, whether a member of staff or a member of the public, knows who to contact;

- Appropriate technical and organisational security measures are in place to safeguard personal data
- Methods of processing personal data are regularly audited and compliance concerns, errors or areas for improvement are acted upon
- Paper files and other records or documents containing personal data are scanned into WriteUpp and shredded/destroyed. No paper files are kept at Talking Lab.
- Data Security Breaches are reported and acted upon in accordance with the Data Security Breach Management Policy and those that are required to be reported to the Information Commissioner's Office (ICO) are passed to them within 72 hours of becoming aware
- Personnel are aware that personal data must not be accessed unless there is a business need to do so and, where a Data Security Breach occurs as a result of them knowingly or recklessly incorrectly or inappropriately processing personal data, this constitutes a breach of the Act, the UK GDPR, this policy and the Council's Code of Conduct for which they will be personally liable.

Appendix 1

Lawful Bases and Conditions for Processing

The lawful bases for processing personal data are set out in Article 6 of the UK GDPR. At least one of these must apply whenever personal data is processed:-

- Consent the individual has given clear consent for you to process their personal data for a specific purpose.
- Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
- Vital interests: the processing is necessary to protect someone's life.
- Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

If **special category data** is to be processed, both a lawful basis for processing and a special category condition for processing in compliance with Article 9 of the UK GDPR must be identified and documented

- Explicit Consent: the data subject has given explicit consent to the processing of the personal data for one or more specified purposes.

- Carrying out employment, social security and social protection obligations: The processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.
- Vital Interests: Where the subject lacks capacity, processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.
- Political, Philosophical, Religious or Trade Union Aims: Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.
- Personal Data made public by the Data Subject: processing relates to personal data which are manifestly made public by the data subject.
- Defence of Legal Claims: processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
- Substantial Public Interest: processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
- Preventive or Occupational Medicine: processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3.
- Public Health: processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.
- Archiving: processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Appendix 2

The Caldicott Principles

The Caldicott Principles govern the use of information within Health and Social Care but are equally relevant in all areas of our work, ensuring the minimum amount of personal data is exchanged, and only when absolutely necessary. They are:-

1. Justify the purpose(s)

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

2. Don't use personal confidential data unless it is absolutely necessary

Personal confidential data should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3. Use the minimum necessary personal confidential data

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data transferred or accessible as is necessary for a given function to be carried out.

4. Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

5. Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data – both clinical and non-clinical staff – are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. Comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

7. The duty to share information can be as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Reviewed on 24/01/2024 by Lucy Darby

Next review due by: 24/01/2025