INFORMATION AND DATA SECURITY PROTECTION POLICY FOR THE KELLY FOUNDATION.

1. Introduction

1.1. This Data Security Policy covers the safeguarding and protection of sensitive personal information and confidential information as is required by law (including, but not limited to, the Data Protection Act 2018, Health & Social Care Act 2012, and the Common Law duty of confidentiality) and is intended to comply with all the requirements of ISO 27001 in so far as the responsibility to protect personal confidential is concerned.

2. Purpose

2.1. The purpose of this document is to outline how we prevent data security breaches and how we will react to them when prevention is not possible. By data breach we mean a security incident in which the confidentiality, integrity or availability of data is compromised. A breach can either be purposeful or accidental.

2.2. This Data Security Policy covers:

2.2.1. Physical Access procedures;

2.2.2. Digital Access procedures;

2.2.3. Access Monitoring procedures;

2.2.4. Data Security Audit procedures;

2.2.5. Data Security Breach procedures.

3. Scope

3.1. The policy includes in its scope all data which we process either in hardcopy or digital copy.

3.2. This policy applies to all staff, including temporary staff and contractors.

4. Physical Access Procedures

4.1. Physical access to records will be granted on a strict 'Need to Know' basis.

4.2. During induction each staff member who requires access to confidential information will be trained on the safe handling of all information and will be taught the procedures which govern how data is used, stored, shared and organised in The Kelly Foundation.

4.3. Our staff will retain personal and confidential data securely in locked storage and when not in use and keys will not be left in the barrels of filing cabinets or doors.

4.4. **Data is stored at the Foundation office in Pinetrees.** Our office, when left unoccupied, will be locked unless all personal and confidential information has first been cleared off work stations/desks and secured in locked storage.

4.5. We will risk assess each storage location to ensure that the data is properly secured.

4.6. A record will be kept of who has access to the storage location. This record can be found in the security log kept by the General Manager.

4.7. An audit will be completed at least annually to ensure that information is secured properly and that access is restricted to those who have a legal requirement to use the information. The details of this audit are outlined in the Data Security Audit Procedures [7] below.

5. Digital Access Procedures

5.1. Access shall be granted using the principle of 'Least Privilege'. This means that every program and every user of the system should operate using the least set of privileges necessary to complete their job.

5.2. We will ensure that each user is identified by a unique user ID so that users can be linked to and made responsible for their actions.

5.3. During their induction each staff member who requires access to digital systems for their job role will be trained on the use of the system, given their user login details, and they will be required to sign to indicate that they understand the conditions of access.

5.4. A record is kept of all users given access to the system. This record can be found in the General Manager user log.

5.5. In the instance that there are changes to user access requirements, these can only be authorised by the General Manager.

5.6. The General Manager user log will contain the location of all confidential and sensitive personal information which is digitally stored.

5.7. We will follow robust password management procedures and ensure that all staff are trained in password management.

5.8. As soon as an employee leaves, all their system logons will be revoked.

5.9. As part of the employee termination process the General Manager is responsible for the removal of access rights from the computer system.

5.10. The General Manager will review all access rights on a regular basis, but in any event at least once a year. The review is designed to positively confirm all system users. Any lapsed or unwanted logons which are identified are disabled immediately and deleted unless positively reconfirmed.

5.11. When not in use all screens which have access to confidential data will be locked and a clear screen policy will be followed.

6. Access Monitoring Procedures

6.1. The management of digital access rights is subject to regular compliance checks to ensure that these procedures are being followed and that staff are complying with their duty to use their access rights in an appropriate manner.

6.2. Areas considered in the compliance check include whether:

6.2.1. Allocation of administrator rights remains restricted.

6.2.2. Access rights are regularly reviewed.

6.2.3. Whether there is any evidence of staff sharing their access rights; **(staff should know that this can result in disciplinary procedures as sharing access is not permitted)**

6.2.4. Staff are appropriately logging out of the system;

6.2.5. Our password policy is being followed;

6.2.6. Staff understand how to report any security breaches.

7. Data Security Audit Procedures

7.1. Confidentiality audits will focus on controls within electronic records management systems and paper record systems; the purpose being to discover whether confidentiality has been breached, or put at risk through deliberate misuse of systems, or as a result of insufficient controls. Audits of security and access arrangements within each area are to be conducted on a 12 monthly basis

7.2. Audits will be carried out as required by some or all of these methods:

7.2.1. Interviews with management and staff. These audits will be carried out by an external auditor appointed for the task

7.2.2. Based on electronic reports as the auditor deems fit

7.2.3. Based on electronic reports from care planning software or auditing of care plans as the auditor deems fit**.**

7.3. The following checks will be made during data annual security audits:

7.3.1. The Information in the Security User Log has been reviewed, updated and signed off;

7.3.2. The Record of Processing Activities has been reviewed, updated and signed off;

7.3.3. Failed attempts to access confidential information identified;

7.3.4. Repeated attempts to access confidential information identified;

7.3.5. Access of confidential information by unauthorised persons;

7.3.6. Previous confidentiality incidents and actions, including disciplinary, taken;

7.3.7. Staff awareness of policies and guidelines concerning confidentiality and understanding of their responsibilities with regard to confidentiality;

7.3.8. Appropriate recording and/or use of consent forms;

7.3.9. Appropriate allocation of access rights to confidential information, both hardcopy and digital;

7.3.10. Storage of and access to filed hardcopy service user notes and information;

7.3.11. Appropriate use and security of desktop computers and mobile devices in open areas;

7.3.12. Security applied to PCs, laptops and mobile electronic devices;

7.3.13. Evidence of secure waste disposal;

7.3.14. Appropriate transfer and data sharing arrangements are in place;

7.3.15. Security and arrangements for recording access to manual files both live and archive, *e.g.* storage in locked cabinets. Appropriate staff use of computer systems, *e.g.* no excessive personal use, no attempting to download software without authorisation, use of social media.

8. Data Security Breach Procedures

8.1. In order to mitigate the risks of a security breach we will:

8.1.1. Follow the Physical Access, Digital Access, Access Monitoring and Data Security Procedures;

8.1.2. Ensure our staff are trained to recognise a potential data breach whether it is a confidentiality, integrity or availability breach;

8.1.3. Ensure our staff understand the procedures to follow and how to escalate a security incident to the correct person in order to determine if a breach has taken place.

8.2. In the instance that it appears that a data security breach has taken place:

8.2.1. The staff member who notices the breach, or potential breach, will advise the General Manager who will prepare a report within 8 hours;

8.2.2. The General Manager will also conduct a thorough investigation into the breach;

8.2.3. In the instance that the breach is a personal data breach and it is likely that there will be a risk to the rights and freedoms of an individual then the Information Commissioner's Office (ICO) will be informed as soon as possible, but at least within 72 hours of our discovery of the breach, via the DSPT Incident Reporting Tool (www.dsptoolkit.nhs.uk/incidents/);

8.2.4. As part of our report we will provide the following details:

8.2.4.1. The nature of the personal data breach (i.e. confidentiality, integrity, availability);

8.2.4.2. The approximate number of individuals concerned and the category of individual (e.g. employees, mailing lists, service users);

8.2.4.3. The categories and approximate number of personal data records concerned;

8.2.4.4. The name and details of our General Manager who is responsible for Data Protection;

8.2.4.5. The likely consequences of the breach;

8.2.4.6. A description of the measures taken, or which we will take, to mitigate any possible adverse effects.

8.2.5. The General Manager will inform any individual that their personal data has been breached if it is likely that there is a high risk to their rights and freedoms. We will inform them directly and without any undue delay;

8.2.6. A data security breach must be marked on the Information Security Log and will prompt an external audit of all processes in order to correct any procedure which led to the breach;

8.2.7. A record of all personal data breaches will be kept including those breaches which the ICO were not required to be notified about.

9. Responsibilities

9.1. **Emma Rees** is responsible for physical security;

9.2. **Emma Rees** is responsible for updating and auditing the relevant Log;

9.3. **Emma Rees** is responsible for digital access;

9.4. **Emma Rees** is responsible for managing breaches;

9.5. **External Auditor** is responsible for data security audits.

10. Approval

10.1. This policy has been approved by the Trustees and the Chairman and will be reviewed at least annually.

Name	JOHN STOOKE
Signature	John A Stooke
Approval Date	23 July 2023
Review Date	1 August 2024