Data Security Policy

1. Introduction

1.1. This Data Security Policy is ***Holbrook Halls*** (hereafter referred to as "us", "we", or "our") policy as regards 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).

2. Purpose

2.1. The purpose of this document is to outline how we prevent data security breaches and how we 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 breach procedures.

3. Scope

3.1. This policy includes in its scope all data which is stored, recorded or transferred and of which we can reasonably be stated to be either the data controller or data processor, this includes special categories of data.

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

4. Physical Access Procedure

4.1. Physical access to records shall only be granted on a strict ‘Need to Know’ basis.

4.2. During their induction each staff member who requires access to confidential information for their job role 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 our organisation.

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

4.4. All offices, when left unoccupied, must be locked unless all personal and confidential information has first been cleared off work stations/desks and secured in locked storage

4.5. The Information Asset Register (IAR) will contain the location of all confidential and sensitive personal information.

4.6. We will risk assess each storage location to ensure that the data is properly secured. This risk assessment forms part of the IAR.

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 Access Monitoring Procedures [6] below.

5. Digital Access Procedure

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. The use of group IDs is only permitted where they are suitable for the work carried out

5.4. 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;

5.5. A record is kept of all users given access to the system. This record can be found ***Insert location here***;

5.6. In the instance that there are changes to user access requirements, these can only be authorised by the Data Security and Protection Lead.

5.7. The IAR will contain the location of all confidential and sensitive personal information which is digitally stored;

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

5.9. When not in use all screens will be locked and a clear screen policy will be followed.

6. Access Monitoring Procedures

6.1. The management of access rights is subject to regular compliance checks to ensure that this procedure is 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 is restricted;

6.2.2. Access rights are regularly reviewed;

6.2.3. There is any evidence of staff sharing their access rights;

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 Breach Procedures

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

7.1.1. Follow the Physical Access, Digital Access and Access Monitoring Procedures;

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

7.1.3. We 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;

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

7.2.1. The staff member who notices the breach, or potential breach, will complete a Data Security Breach Incident Report Form;

7.2.2. This form will be completed and handed to the Data Security and Protection Lead or, if they are not available, to a member of senior management;

7.2.3. The Data Security and Protection Lead will complete the rest of the Incident Report Form and conduct a thorough investigation into the breach;

7.2.4. 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 via their website: https://ico.org.uk/for-organisations/report-a-breach/;

7.2.5. As part of our report we will provide the ICO with the following details:

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

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

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

7.2.5.4. The likely consequences of the breach;

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

7.2.6. The Data Security and Protection Lead 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;

7.2.7. A data security breach must be marked on the IAR and will prompt an audit of all processes in order to correct any procedure which led to the breach.

8. Responsibilities

8.1. **The management team** is responsible for physical security;

8.2. **The management team** is responsible for updating and auditing the IAR;

8.3. **The management team** is responsible for digital access;

8.4. **The management team** is responsible for managing breaches;

9. Approval

9.1. This policy has been approved by the undersigned and will be reviewed at least annually.

Name	Gavin Vaughan
Signature	
Approval Date	
Review Date	