



---

# Hunts Mind Data Protection Policy

---

Ratified by the Board of Trustees:-  
**17<sup>th</sup> August 2011**

To be reviewed:-  
**August 2014**  
or as legislation changes

**The Limes  
24, New Street  
St Neots  
Cambridgeshire PE19 1AJ**

**Registered Charity number 1084452  
Company Limited by guarantee 3949645**



## Data Protection Policy

### Introduction

Hunts Mind needs to keep certain information about its employees, volunteers, members and service users to allow it to monitor performance, achievements, health and safety and other statutory requirements. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, Hunts Mind must comply with the eight Data Protection Principles, which are set out in the Data Protection Act 1998<sup>1</sup>. In summary these state that personal data shall:

- be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met
- be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose
- be adequate, relevant and not excessive for those purposes
- be accurate and kept up to date
- not be kept for longer than is necessary for that purpose
- be processed in accordance with the data subject's rights
- be kept safe from unauthorised access, accidental loss or destruction and
- not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

Important Note: The Data Protection Act 1998 extends the scope of legislation to include written and printed etc. material, not just the electronic data.

Hunts Mind and all of its staff, or others who process or use any personal information, must ensure that they follow these principles at all times. In order to ensure that this happens, Hunts Mind has developed this Data Protection Policy.

### What is defined as personal data?

Personal data is defined in the Act, at Section 1(1), as follows:

“data which relates to a living individual who can be identified: from those data; or from those 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”.

However the Information Commissioner would advise caution in working only to this limited definition and we would refer you to section 2 of the following:

---

<sup>1</sup> <http://www.legislation.hmsso.gov.uk/acts/acts1998/19980029.htm>



[http://www.ico.gov.uk/upload/documents/library/data\\_protection/detailed\\_specialist\\_guides/data\\_protection\\_act\\_legal\\_guidance.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf) for further detail.

## **Status of the policy**

This policy is incorporated in Hunts Mind formal contract of employment. Infringement of the requirements of this policy may result in disciplinary action being taken. If any Hunts Mind staff, volunteers, members or service providers consider that this Policy has not been followed, in respect of personal data about themselves, should raise the matter initially with the designated Data Controller. If the matter is not resolved it should be raised as a formal grievance.

## **Responsibilities of staff**

All staff are responsible for:

- checking that any information that they provide to Hunts Mind in connection with their employment is accurate and up to date
- informing Hunts Mind of any changes to information which they have provided, e.g. changes of address and
- informing Hunts Mind of any errors or changes in staff information.

If and when, as part of their responsibilities, staff collect information (i.e. personal information, opinions about ability, or details of personal circumstances) about other people or members, they must comply with any guidelines which may be published. In particular, they must seek the permission of the Data Controller for their proposed information collection and uses.

The Chief Executive has overall responsibility and is responsible for monitoring the steps taken to ensure that the Act and this Policy are complied with. Particular care must be taken when work is being undertaken externally or when an existing body of material is being brought within Hunts Mind for the first time.

## **Data security**

All staff are responsible for ensuring that:

- 1 Any personal data, which they hold, or for which they are responsible, is kept securely, for example:
  - Kept in a locked filing cabinet;
  - In a locked drawer;
  - If it is computerised, be password protected
  - If computerised, then the computer itself is kept in suitably secure conditions. Data should not be stored on the hard drives of desktop personal computers but on the networked storage facilities provided.



- Where it is necessary to store information on laptop computers (or off-site) then the machine must at all times be maintained physically secure. Where the data is particularly sensitive, consideration must be given to the adoption of additional security measures which would protect the information in the event of the loss or theft of the computer. Care must be taken to ensure that data is frequently transferred to network storage and that discrepancies are not allowed to arise.
  - Where information is to be gathered through, or used on, a website then appropriate measures must be in place to control access and prevent unauthorised disclosure.
- 2 Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.

Advice on the collection, retention and secure storage of information may be obtained from the Data Controller.

Staff should note that unauthorised disclosure is a breach of the Data Protection Act and may result in disciplinary action. In some cases it may be considered as gross misconduct. It may also result in a personal liability for the individual staff member.

### **Rights to access information (S.A.R.s)**

Employees and other users of Hunts Mind have the right to access any personal data that is being kept about them either on computer or in certain files. Should any person wish to exercise this right they should contact the Data Protection Controller. In order to gain access a request should be made in writing to the Data Protection Controller.

Hunts Mind reserves the right to make a charge of up to £10 on each occasion that access is requested.

Hunts Mind aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days.

### **Subject consent**

In many cases, Hunts Mind can only process personal data with the consent of the individual. In some cases, if the data is sensitive, express consent must be obtained. Agreement to Hunts Mind processing some specified classes of personal data is a condition of employment for staff. This includes information about previous criminal convictions in accordance with the Rehabilitation of Offenders Act 1974.

Therefore, all prospective staff will be asked to consent to their data being processed when an offer of employment is made.



## **Processing sensitive information**

Sometimes it is necessary to process sensitive information about a person such as race, gender or family details. This is done to ensure that Hunts Mind can operate policies on matters such as sick pay or equal opportunities. Hunts Mind may also ask for information about particular health needs or disabilities. Hunts Mind will only use such information in the protection of the health and safety of the individual, but will need consent to process - for example, in the event of a medical emergency. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, employees and others affected will be asked to give express consent for Hunts Mind to do this.

## **The Data Controller**

The designated Data Controller will deal with the implementation of agreed policy and day to day matters.

Hunts Mind has a designated Data Controller. In their absence, the Chair of the Board of Trustees may be consulted.

Hunts Mind's designated Data Controller is the Chief Executive.

## **Retention of data**

Hunts Mind will keep some forms of information for longer than others.

Hunts Mind will need to keep central personnel records for 6 years after employment ceases. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references. Retention of all other documents and paperwork are detailed on Appendix A.

## **Conclusion**

Compliance with the Data Protection Act 1998 is the responsibility of all members of Hunts Mind. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or access to Hunts Mind's facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this Policy should be taken up with the Data Controller.

Hunts Mind



For better  
mental health

## **Hunts Mind Data Protection Policy**

**Date policy ratified by Executive Committee: 17<sup>th</sup> August 2011**

**Signature of Chair:**

A handwritten signature in black ink, appearing to be "S. Lee".

**To be updated: August 2014 – unless legislation changes**



## Appendix A

### Personnel records – retention periods

The recommended retention periods (non-statutory) are based on the six-year limit, the legal proceedings must be commenced under the Limitation Act 1990. Thus where files/documents may be relevant to a contractual claim these must be retained for the corresponding six year limitation period.

In the event that employment contracts/accident record books and other personnel records are needed for the purpose of a legal action, the originals must be made available or the employer must explain what happened to the original documents backed up by what is known as a 'statement of truth'.

Record type	Retention period	Legal requirement
Application forms and interview notes for unsuccessful candidates.	6 months	N/A
Personnel files	6 years after employment ceases.	N/A
Redundancy details, calculations of payments, notifications to the Secretary of State	6 years from the date of redundancy.	
Senior Executive records	Permanently	
Trade Union agreements	10 years after ceasing to be effective.	
Joint Negotiating Minutes	Permanently	
Statutory maternity pay records, calculations, certificates or other medical records	3 years after the end of the tax year in which the maternity period ends.	The Statutory Maternity Pay Regulations 1986 (SI 1986/1960)
Statutory Sick Pay records, calculations, certificates, self-certificates	3 years after the end of the tax year to which they relate.	The Statutory Sick Pay (General) Regulations 1982 (SI 1982/894) as amended
Income Tax and NI returns, income tax records and correspondence and correspondence with HM Revenue & Customs	Not less than 3 years after the end of the financial year to which they relate.	The Income Tax (Employments) Regulations 2003 (1993/744) as amended, for example by The Income Tax (Employments) (Amendment No. 6) Regulations 1996 (SI 1996/2631)
Wages/salary records (inc. overtime, bonuses and expenses).	Not less than 3 years after the end of the year to which they relate.	Taxes Management Act 1970
Accident books, accident records/reports	3 years after the date of the last entry.	1995 (RIDDOR) (SI 1995/3163) as amended
Trustees' minute books	Permanently	