Hillingdon Brain Tumour Group

DATA PROTECION PROCEDURE

Last Review:	March 2018
Update By:	March 2020
Approved By Chair:	March 2018

Registered Charity No. 1164538

Data Protection Procedure

Purpose of this procedure
This procedure supports the Hillingdon Brain Tumour Group Information Governance Policy and defines data protection from a Hillingdon Brain Tumour Group perspective which includes what the law requires in this respect (Data Protection Act 1998). It describes the processes to follow to ensure that all employees are able to support and comply with standards of data protection.

This procedure is one of a suite of procedures which support the Information Governance Policy including:

- The Data Protection Policy
- Confidentiality Policy
- Confidentiality Code of Conduct
- Records Management Procedure
- Information Breach Procedure
- Customer Relations Management Procedures (CRM)

In addition this procedure is closely aligned to the Risk Register and the Business Continuity Plan.

Scope

The scope of this procedure extends to all areas of the business where personal information is captured and retained for any purpose by Hillingdon Brain Tumour Group. It defines what the term "personal information" includes and explains the rights and responsibilities of those people for whom Hillingdon Brain Tumour Group retain information as well as of all Hillingdon Brain Tumour Group' employees and volunteers.

This subject is significant and so for ease we have split the procedure into sections:

Section 1) Introduction

1.1 What is data?
1.2 Why do we need to protect it?
1.3 Who is responsible for Information and Data within Hillingdon Brain Tumour Group?

Section 2) The Data Protection Act

2.1 What is the Data Protection Act?
2.2 What are the common terms used within the Act and what do they mean?
2.3 The 8 principles of the Data Protection Act
2.4 How does the Act apply to Hillingdon Brain Tumour Group?
2.5 How do we comply with the Act?

Section 3) The Information Commissioner's Office (ICO)

3.1 Who are the ICO?
3.2 What is the ICO responsible for?

Section 4) The rights of individuals

4.1 What are the rights of individuals for whom Hillingdon Brain Tumour Group holds information?
4.2 Subject Access Requests

Appendix 1: A guide to complying with the Data Protection Ac

Section 1) Introduction

1.1 What is Data?

The Data Protection Act defines data as meaning information which;

a) Is being processed by means of equipment operating automatically in response to instructions given for that purpose.
b) Is recorded with the intention that it should be processed by means of such equipment.
c) Is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system.
d) Does not fall within a) b) or c) but forms part of an accessible record or
e) Is recorded information held by a public authority and does not fall within any of a) to d)

The words are complex and it is easy to read them and still not understand what they actually mean. Basically we should think about this procedure, the policy it supports and the other procedures within this suite of procedures as referring to any data or information whether it is electronic or paper based as being within scope.

1.2 Why do we need to protect it?

Individuals provide their personal information to Hillingdon Brain Tumour Group because they believe we require this and because they believe that we will keep it confidential. A disclosure of personal information can occur all too easily if we don't have processes in place to prevent this. Once the disclosure or breach has occurred then individuals can find themselves victims of identity theft and fraud; they may be damaged because others know things about them which they shouldn't. This can make individuals vulnerable or expose those who are vulnerable.

Hillingdon Brain Tumour Group, by the very nature of its work, captures information which can be sensitive and so it all too easy to see how dangerous exposing this can be to the individual.

1.3 Who is responsible for Information and Data within Hillingdon Brain Tumour Group?

All employees and volunteers are responsible for our information and ensuring that it is as secure as is possible. However, some individuals have specific responsibilities;

The Chair and Vice Chair are responsible for governance. They develop and monitor the Information Governance Policy and the Chair and Vice Chair monitors the organisation's adherence with this. The Chair and Vice Chair is responsible for supporting the Trustees to review and amend the Policy. The Chair and Vice Chair also reports to the Trustees on data matters including breaches and subject access requests as well as working with the Trustees to monitor the risk register in respect of information security.

The Chair and Vice Chair, Senior Manager and Business Manager maintains the suite of procedures which support the Information Governance Policy ensuring that they are effective in their purpose and that the organisation is compliant.

The Chair and Vice Chair is responsible for data protection and ensuring records management is compliant with our contracts and grants, the Department of Health Guidelines and the Data Protection Act 1998. This post is also responsible for monitoring the effectiveness of procedures and will conduct process reviews and compliance audits.

Internal auditors undertake audits for all our management systems including information governance. They perform this role in addition to their normal duties. These staff maybe employed by the partner organisations.

All Employees and Volunteers have responsibilities to ensure that personal and sensitive information is kept safe and confidential. All employees and volunteers are required to understand and follow the policies and procedures in place within the Hillingdon Brain Tumour Group Information Management System and to alert senior employees if they are concerned about security.

Section 2) The Data Protection Act

2.1 What is the Data Protection Act?

The Data Protection Act 1998 establishes a framework of rights and duties which are designed to safeguard personal data. It seeks to balance the legitimate needs for organisations like Hillingdon Brain Tumour Group and others to collect and use personal data for business and other purposes against the rights of individuals to respect for the privacy of their personal information.

2.2 What are the common terms used within the Act and what do they mean?

- **What does "processing personal information" mean?**

  If you collect or hold information about an identifiable, living individual or if you use, retain, disclose or destroy that information, then you are likely to be processing personal information; therefore the scope for the Data Protection Act is very broad.

- **What is "personal" information?**

Personal information is information captured and/or retained for any period about a living identified or identifiable individual. This includes information such as names and addresses, bank details and opinions expressed about an individual.This includes employees, participants, volunteers, students, clients, funders, commissioners and others who may have disclosed information of this nature to Hillingdon Brain Tumour Group.

What is "sensitive" personal information?

Some types of personal information are classed as being "sensitive". This is where the depth of personal information extends to information about:

- Racial or ethnic origin
- Political opinions
- Religious or other beliefs
- Trade Union membership
- Physical or mental health conditions
- Sexual life
- Offences or alleged offences committed
- Proceedings relating to those offences or alleged offences
- The rules about the capture and retention of personal information which is classed as being "sensitive" are stricter and described within this procedure.

Who is the Data Controller?

Hillingdon Brain Tumour Group is the data controller for the information we hold about our clients, employees, volunteers and others. The Data Protection Act uses the term Data Controller in place of "organisation" or "you".

Who is the Data Subject?

The data subject is the individual whose data or information is held. The Data Protection Act uses the term Data Subject in place of individual.

Data Minimisation

We are required to only hold the information we require for the purpose we require it for; no more, no less. This is called data minimisation. You can read more about this in section 2.5 under principle 3) below.

2.3 The 8 principles of the Data Protection Act

The data protection act describes eight data protection principles:

1) Personal data shall be processed fairly and lawfully;
2) Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose of those purposes;
3) Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
4) Personal data shall be accurate and, where necessary, kept up to date;
5) Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes;
6) Personal data shall be processed in accordance with the rights of data subjects under this Act;
7) Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing or personal data and against accidental loss or destruction of, or damage to, personal data;

8) Personal data shall not be transferred to a country 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 or personal data.

2.4 How does the Act apply to Hillingdon Brain Tumour Group?

The Data Protection Act applies to a particular activity rather than to an individual or an organisation. The particular activity it applies to is "processing personal information". So if Hillingdon Brain Tumour Group or individuals working for or volunteering for it handle personal information, then "The Act" is applicable. This means we all need to handle personal information according to the principles of the act. The principles are described below.

Hillingdon Brain Tumour Group processes personal information and therefore we are registered with the Information Commission on the Data Protection Public Register. This means we have told the Information Commission that we do process personal information and how we do this and they have issued us with registration numbers so they can identify us.

2.5 How do we comply with the Act?

See Appendix 1: A guide to complying with the Data Protection Act

Section 3) The Information Commissioner's Office (ICO)

3.1 Who are the ICO?

The ICO is the UK's independent authority who upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Information Commissioner has responsibilities around the "freedom of information act" as well as data protection.

3.2 What are the ICO responsible for?

The Data Protection Act makes the ICO responsible for;

- Promoting good practice in handling personal data and giving advice and guidance on data protection;
- Keeping a register of organisations who process information and data;
- Helping to resolve disputes to determine if organisations have completed with the Data Protection Act;
- Taking action to enforce compliance where necessary;
- Bringing prosecutions for offences committed under the Act.

Section 4) The rights of individuals

4.1 What are the rights of individuals for whom Hillingdon Brain Tumour Group hold information?

The rights of individuals for whom Hillingdon Brain Tumour Group may hold personal and/or sensitive information are protected under the Data Protection Act 1998. Individuals have certain rights under this law as follows:

Individuals have the right to obtain information held about them.

- **Individuals have a right to ask at any time for Hillingdon Brain Tumour Group not to use their personal information for direct marketing purposes**.

Anyone wishing to make this request should do so in writing to the Chief Executive who will ensure that Hillingdon Brain Tumour Group acts upon this request within 40 days.

- **Individuals have the right to have personal information which is misleading or incorrect held by Hillingdon Brain Tumour Group corrected**.

If an employee/volunteer is responsible for the storage of personal information receives a request for information to be corrected they must ensure that they refer the request directly to the Chair and Vice Chair.

If Hillingdon Brain Tumour Group or its employees fail to act upon such a request, and the information held, is discovered to be inaccurate or misleading the individual has a right to obtain a court order. A court order can direct Hillingdon Brain Tumour Group to correct the information held and subsequently a court may be involved to decide if the information is inaccurate or misleading. In such a case Hillingdon Brain Tumour Group could incur costs including compensation.

Individuals have a right to prevent Hillingdon Brain Tumour Group making decisions about them using only an automated system.

This area is complex and can extend as far as recruitment decisions made entirely by psychometric testing. Hillingdon Brain Tumour Group does not employ any processes within its management system which use solely automated systems to make decisions about individuals. Any complaints or grievances raised in this respect should be referred to the Chair and Vice Chair for advice and guidance

- **Individuals have the right to know if Hillingdon Brain Tumour Group or someone acting on their behalf is processing personal information about them**.

- **Individuals have the right to know what information is being processed, why and who it may be disclosed to**.

- **Individuals have the right to receive information about them.**

- **Individuals have the right to know about the sources of any information about them**

4.2 Subject Access Requests from Hillingdon Brain Tumour Group employees or volunteer

If any employee or volunteer of Hillingdon Brain Tumour Group receives a request for information about themselves even if they do not refer directly to their rights or the act they should refer the request immediately to the Chair and Vice Chair. These requests are called subject access requests or SAR's. Requests will only be considered if they are received in writing including electronically.

The Chair and Vice Chair should take steps to verify the identity of the person making the request. This can be achieved by asking for verification such as a council tax bill or formal identification. The Chair and Vice Chair should consider if they need to clarify specifically what is being asked for if the request is not clear or broad ranging and general. For example if a request to see emails is received they may want to ask what dates the emails were sent or what they refer to etc.

Hillingdon Brain Tumour Group must respond to an SAR within 40 days and should wherever possible include actual copies of documents etc. rather than written references to them. If they feel it is of a disproportionate effort then they may decide to decline the request on this basis.

Any information sent following an SAR should be easy to understand. For example any codes used should be explained.

The Chair and Vice Chair will retain a log of all SAR requests.

4.1 Subject Access Requests from individuals who are not Hillingdon Brain Tumour Group employees or volunteers.

When a non-employee/volunteer makes a subject access request they should do so by contacting the Chair and Vice Chair directly in the first instance. Requests sent to other personnel should be forwarded directly to the Chair and Vice Chair.

The Chair and Vice Chair will acknowledge the request and note the request on the SAR log. The request will then be forwarded to the relevant manager who will deal with the request and provide information to the Chair and Vice Chair to update the log. The Chair and Vice Chair should always make a judgement about the amount of information being requested.

Section 5) Sharing information with a third party

What if a third party asks you to share information?

Sometimes we may be asked by a third party to share information about an individual or group of individuals e.g. the police or another charity. Sometimes this is acceptable and sometimes it is not. Employees and volunteers should not worry about making these decisions. If everyone follows the procedures in place it will be clear when this is acceptable and when it is not.

Our privacy statement details any information we may already know we intend to share and who with so it may be clear from checking this if you should share the data being requested. However, if this is not clear and you are not sure then you must seek approval before sharing the information being requested. Send requests to your Chair and Vice Chair who will review the request and either approve, reject or refer it to the relevant Manager

Top Tip! If you are not sure if you should share information refer to the Chair and Vice Chair.
We would prefer you to check first if you are not sure.

Appendix 1: A Guide to Complying with the Data Protection Act *(this guide is also available as a separate document)*

Principle 1) Personal data shall be processed fairly and lawfully	
What does this mean?	**How can we all ensure we comply with these requirements?**
This means we must: 1.1 Have legitimate grounds for collecting and using the personal data; 1.2 Not use the data in ways that have unjustified, adverse effects on the individuals concerned; 1.3 Be transparent about how we intend to use the data, and give individuals appropriate privacy notices when collecting their personal data; 1.4 Handle people's personal data only in ways they would reasonably expect; and 1.5 Make sure we don't do anything unlawful with the data	The Hillingdon Brain Tumour Group Code of Confidentiality is the first place to start to ensure you are compliant with the Data Protection Act. Hillingdon Brain Tumour Group employees and volunteers can do the following things to ensure we comply; • Only use the forms and templates which are issued to the management system to capture and record information about individuals. This is important because they have been developed to ensure that they do collect the information we need but that we avoid collecting information we don't need for that particular area of our business; • Use our electronic data systems system in preference to paper based systems. Our data holding system has been established using the same principles as outlined above for paper based systems so we know we are only collecting the right amount of information; • Only store paper based records according to our records management procedure which will inform you how to store information, where and for how long as well as how to dispose of it; • Only transport paper based records according to our records management procedure;

Principle 2) Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose of those purposes	
What does this mean?	**How can we all ensure we comply with these requirements?**
This means that we must: • Be open with individuals as to why we are obtaining the information and what we will do with the information after we have collected it. We must also ensure that if we decide to use the information for something different than the purpose we initially declared, then we must seek the permission of the individual first. • It also means that we must ensure we comply with everything requested of us by the Information Commissioner. • In summary, before we collect any information about an individual we must make sure we are clear with them what information we are collecting and why, what we intend to do with it, including if we intend to share it. If we want to change any of this later we generally will need to seek the permission of the individual.	The Hillingdon Brain Tumour Group Code of Confidentiality is the first place to start to ensure you are compliant with the Data Protection Act. • Use the privacy statements in place according to the Privacy Statements Procedure. This ensures that we are giving individuals all the information they need about how and why we will collect information and what we will do with it. • The Chair and Vice Chair is responsible for ensuring that our registration with the ICO is appropriately maintained and also for alerting them to any data breaches according to the Hillingdon Brain Tumour Group Information Breach Procedure. By maintaining our registration with the ICO we are making them aware of the information we are collecting and why. We review our registration with the ICO annually in line with the review of this procedure and associated policies and procedures.
Principle 3) Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.	
What does this mean?	**How can we all ensure we comply with these requirements?**
This means that we: • Must hold information about an individual that is sufficient for the purpose we are holding it for and in relation to that individual. It also means that we must not hold more information that we need for that purpose. • We are required to identify the minimum amount of information we require to fulfil our purpose and only collect and hold this.	• The Hillingdon Brain Tumour Group Code of Confidentiality is the first place to start to ensure you are compliant with the Data Protection Act. • Hillingdon Brain Tumour Group employees and volunteers can do the following things to ensure we comply; • Only use the forms and templates which are issued within the data management system to capture and record information about individuals. This is important because they have been developed to ensure that they do collect the information we need but that we avoid collecting information we don't need for that particular area of our business;

	Use the CRM system in preference to paper based systems. Our CRM system has been established using the same principles as outlined above for paper based systems so we know we are only collecting the right amount of information.
Principle 4) Personal data shall be accurate and, where necessary, kept up to date.	
What does this mean?	**How can we all ensure we comply with these requirements?**
This means that we must ensure we take reasonable steps to: Ensure we take reasonable steps to ensure that the accuracy of any personal information given to us and that we record where we received the information from. Consider all requests to update information and whether it is necessary for us to do so.	The Hillingdon Brain Tumour Group Code of Confidentiality is the first place to start to ensure you are compliant with the Data Protection Act. Ensure our records are updated when customers, employees and volunteers advise that their personal details have changed e.g. change of address etc. Update our records about customers to record any services delivered or interactions which have taken place. Ensure that information provided from another source is checked and verified wherever possible. If information is just rumour but you feel you ought to record it then you should record that it is rumour and its source. In the same way if you are recording your opinion about an individual (for example in a care setting) then you must be clear that it is your opinion. Opinions and rumours are still accurate as long as they are recorded as being opinions or rumours.

Principle 5) Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes;	
What does this mean?	**How can we all ensure we comply with these requirements?**
This means we must ensure; □ we review how long we retain personal data; □ we consider the purpose or purposes we hold the information in order to decide how long we retain it; □ we delete information safely and securely; □ we archive information securely and for appropriate periods of time	The Hillingdon Brain Tumour Group Code of Confidentiality is the first place to start to ensure you are compliant with the Data Protection Act. □ Hillingdon Brain Tumour Group has developed a records management procedure as part of the suite of procedures supporting the Information Governance Policy. Adhering to this procedure will ensure that you are complying with this principle. Our Records Management Procedure takes account of the requirement of contracts, legal requirements and other factors and has considered the retention period for all our information. It may be different for different things so make sure you check. □ Don't store information outside of the specified system. We can't control information if it is not held within our recognised systems. □ We have introduced information governance audits and we will routinely audit how well we are complying with our procedures. We will also consider how effective our procedures are routinely. You can help us to improve our procedures by contributing to consultations and letting us know if things are not working for you. Please don't introduce local systems.

Principle 6) Personal data shall be processed in accordance with the rights of data subjects under this Act.	
What does this mean?	**How can we all ensure we comply with these requirements?**
Individuals have a right to access a copy of the information we hold about them. They have a right to object to the way we are processing their information as well as to prevent us using their information for direct marketing. If an individual believes the information we hold about them is inaccurate then they have a right to ask us to delete or remove it. We may decide that this is not appropriate so it's not straight forward as it may seem. Individuals have a right to claim compensation from us if they feel they have been damaged by a breach of the Act.	The Hillingdon Brain Tumour Group Code of Confidentiality is the first place to start to ensure you are compliant with the Data Protection Act. It is important that access to personal information is not granted by an individual employee or volunteer because an individual asks to see this. All requests from any individual to amend or have a copy of the personal data Hillingdon Brain Tumour Group holds should be sent in the first instance to the Chair and Vice Chair. If requests are sent to other employees or volunteers they should forward them directly to the Chair and Vice Chair. Section 4 above details the process for this.

Principle 7) Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing or personal data and against accidental loss or destruction of, or damage to, personal data	
What does this mean?	**How can we all ensure we comply with these requirements?**
This means that: - We must have security which is appropriate for the nature of personal information we hold. - We are required to be clear about who is responsible for information within the organisation. - We are required to have appropriate policies and procedures in place and to ensure our employees and volunteers are reliable and well trained. - We must ensure that we are always ready to respond to a breach of security swiftly and effectively.	The Hillingdon Brain Tumour Group Code of Confidentiality is the first place to start to ensure you are compliant with the Data Protection Act. - We can all ensure we comply by making sure we follow the processes in place and using the systems provided. - Everyone is responsible for ensuring that only authorised staff and volunteers have access to information. - The Hillingdon Brain Tumour Group Information Governance Policy details who is responsible for Information Governance. Within this procedure these responsibilities are further clarified. - It is important that employees and volunteers attend training and apply this learning within their day to day work. - Hillingdon Brain Tumour Group has detailed procedures in place as well as a well-developed corrective action process. This means that when things go wrong we quickly identify what has gone wrong and strive to improve our processes to prevent reoccurrences. To make the most of this it is important that employees and volunteers are alert to things which go wrong and report them using the appropriate procedures. - Employees and volunteers are urged to raise concerns and

POLICY INFORMATION / AMENDMENT TRACKING FORM

Date of Review	Name of reviewer	Reviewer's comments and recommended changes	Changes agreed (date)	Document updated (date)