Huntington's Disease Association

Data protection policy

Issue date:	June 2022
Version number:	3
Review date:	June 2023
Status:	Approved

Data protection policy

Introduction

The Huntington's Disease Association takes the privacy of our beneficiaries, supporters, members, volunteers and employees very seriously and we are committed to protecting and keeping any personal information protected and stored safely.

Personal information or data is defined as information relating to an individual who can be identified either directly or indirectly from the information provided. Sensitive personal information is classed as data about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, genetic information, biometric information, or information concerning an individual's health, sex life or sexual orientation, often referred to as special categories of personal data

The information we collect allows us to learn more about those who use and support the charity, to take their needs and experiences into account to make more informed decisions and ultimately to improve the quality of life of those affected by Huntington's disease.

This policy sets out how we will comply with the General Data Protection Regulation (GDPR) and the Data Protection Act (2018). As well as comply with the principles that seek to protect personal information that we process from our supporters, volunteers, staff and all those affected by Huntington's disease. Its purpose is also to ensure that we understand and comply with the legislation governing the processing, use and deletion of personal information which we access during the course of our work.

Scope

This policy applies to all people working for the Huntington's Disease Association or on behalf of the Huntington's Disease Association in any capacity, including employees, trustees, agency workers, seconded workers, volunteers, contractors and suppliers.

Our commitment

The Huntington's Disease Association is committed to complying with the data protection principles when processing personal information. This means that:

- We will process personal information lawfully, fairly and in a transparent manner.
- We will only collect personal information for specified, explicit and legitimate purposes, and will not process in a way that is not compatible with these purposes.

- We will only process personal information that is adequate, relevant and necessary for the purpose it was first given.
- We will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information is deleted or corrected without delay.
- We will keep personal information in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the information is processed.
- We will take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.
- We will make sure that any personal information provided to us is accessed only by appropriately trained staff, approved volunteers (e.g. Branch and Support group leads as appropriate) and approved contractors. We will ensure that any external contractors we use are comprehensively checked and adhere to a formal contract or agreement in which our expectations and requirements regarding the way in which they manage, collect and access any personal data, are met.
- We will only disclose personal information when obliged to by law, or the disclosure is necessary for purposes of national security, taxation and criminal investigation, or if we have permission to share personal information. We will only disclose personal information in other circumstances where there is a significant risk to either the person or other persons should the information not be shared.

The Huntington's Disease Association, as the data controller, will be responsible for, and able to demonstrate, compliance with these principles on request.

The personal data that we collect

The Huntington's Disease Association collects personal information for a number of reasons:

- Supporting those affected by Huntington's disease
  To help deliver our services where necessary we collect personal information, including sensitive personal data about health and genetics, when we receive and respond to an enquiry or when people attend one of our events. This information helps us to provide the most effective and appropriate support, advice and guidance.

  Huntington's Disease Association volunteer led branches and support groups also collect personal information about members of their group in order to deliver local peer support services and offer welfare grants to people affected by Huntington's in their local area.
- Supporters
  Where an individual for example, makes a donation, registers to fundraise, signs up for an event or purchases an item from the Huntington's Disease Association shop

we may need to collect personal information such as name, date of birth, email address, postal address, telephone number and banking details to process their interaction appropriately.

- Volunteers
  Where an individual volunteers for the Huntington's Disease Association we may need to collect personal information relevant to their role such as name, date of birth, email address, postal address, telephone number, any conflicts of interests, their connection to Huntington's disease where relevant and disclosure and barring check results where relevant to enable them to carry out their role.
- Data about children
  Where anyone under the age of 18 accesses support through the Huntington's Disease Association we collect the same sensitive information about their health and support needs as we do for any adults we support. We will obtain the permission of parents or guardians before collecting this personal information about a child and will provide children with the same rights and controls over the personal information that we hold on them as we would with adults.
- Keeping informed and direct marketing
  Where consent has been provided, we aim to inform people about the progress the charity is making, keeping them informed of events and activities and periodically we may request support for the Huntington's Disease Association's work or to inform supporters about ways they can support the charity in the future. Any direct marketing undertaken will comply with the rules set out in data protection legislation and the Privacy and Electronic Communications Regulations (PECR).
- Understanding our supporters
  The Huntington's Disease Association will analyse the personal information that is provided to us to help create a profile of our supporters and their preferences so that we only communicate in the most appropriate way and with the most relevant information.
- Membership
  The Huntington's Disease Association collects information on individuals, professionals and organisations who have applied for membership of the charity. We only hold the minimum amount of information that is required to process the membership application and fulfil the obligations of the contractual agreement.
- Staff
  The Huntington's Disease Association collects personal information on those who are employed by the charity as part of their terms and conditions of employment.

Lawful basis for processing personal information

We will only process personal information where an appropriate legal basis for its processing has been identified and communicated. There are six lawful basis for the processing of personal information that the charity may use and a brief explanation of these is outlined below:

- Legitimate interest
  The processing is necessary for the legitimate interest of the charity or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data that overrides those legitimate interests.
- Consent
  The individual has given consent (such as saying YES or ticking an OPT-IN box) for the charity to process their personal information for a specific purpose. Silence or failure to respond does not constitute consent.
- Contract
  The processing is necessary for a contract that the charity has with an individual or because of the specific steps that the charity must take prior to entering a contract.
- Legal obligation
  The processing is necessary to comply with the law (not including contractual obligations).
- Vital interests
  The processing is necessary to protect the individual's vital interests or to protect someone's life.
- Public task
  The processing is necessary for the charity to perform a task which is in the public interest or for an official function which has a clear basis in law.

As part of the Huntington's Disease Association's commitment to strong governance and accountability in the protection of personal information and data we will record our decisions on the identification of the lawful basis for processing information in the relevant privacy statements. We will review these decisions and amend our policies and procedures to reflect any required changes in accordance with the review dates set for the documentation and when legislative changes occur.

The rights of the individual

In accordance with data protection legislation, individuals have the following rights:

- The right to be informed
  An individual has the right to be informed about the collection and processing of their personal information.
- The right of access
  An individual has the right to access their personal information via a subject access request. Requests for access to personal information can be made either verbally or in writing and the information requested will be provided freely unless the request is manifestly unfounded or excessive. There will be no charge levied and where appropriate information will be provided within twenty working days.

- The right to rectification
  An individual has the right to request that inaccurate personal information is rectified, or completed if it is incomplete.
- The right to erasure
  An individual has the right for their personal information to be erased. This is also referred to as `the right to be forgotten'.
- The right to restrict processing
  An individual has the right to restriction or suppression of their personal data and when this processing is restricted, we are permitted to store the personal information but not use it.
- The right to data portability
  Where data is processed by automated means, individuals will be entitled to re-use that information for their own purposes across different platforms.
- The right to object
  Individuals can object to the processing of their personal information. However, the extent of this right depends on the processing purpose.
- Rights related to automated decision making, including profiling
  Where decisions and profiling of personal information are undertaken without human involvement the individual has the right to challenge these decisions and request that they are reviewed.

Third party service providers and suppliers

In those circumstances where the Huntington's Disease Association uses an external or third-party organisation to process personal information on our behalf, we will take additional security measures to ensure that this personal information is safe and not at risk of unauthorised disclosure or loss. The Huntington's Disease Association has in place both contracts and agreements with third party service providers and suppliers to ensure the following:

- That they only act on the written instructions of the Huntington's Disease Association.
- The processing of the personal data is subject to a duty of confidence.
- Appropriate measures are in place to ensure the security of the data.
- That they will assist the charity in providing subject access and enabling individuals to exercise their rights under data protection legislation.
- They will assist the Huntington's Disease Association in achieving ongoing compliance with data protection legislation in relation to security of processing, notification of data breaches and the undertaking of data protection impact assessments and privacy impact assessments.
- At the end of contract, they will delete or return all personal information to the Huntington's Disease Association within specified time parameters.

- They will submit to audits and inspections where necessary to the Huntington's Disease Association on request to evidence ongoing compliance with the data protection obligations and will inform us if they are asked to do anything that is likely to infringe data protection regulations.

Protecting personal information and data

Data accuracy

The Huntington's Disease Association has adopted robust governance of personal information to prevent loss, disclosure and unwarranted destruction.

It is the responsibility of all staff and volunteers, who have access to personal information, to ensure that service user and supporter communication preferences are honoured and respected and that the individual understands how their information will be processed.

When recording the communication preferences of supporters, special attention will be given to electronic communication and email address information will only be used where the individual is happy to be contacted by email for future correspondence.

Where personal information is collected, it is the responsibility of all staff to ensure that this information is complete, up to date, accurate and fit for purpose. In addition, annual data reviews will be undertaken.

We will only collect the minimum amount of personal information required to undertake the task for which the personal information has been provided.
Where personal information is processed, we will ensure that a lawful basis for processing this information has been identified and documented.

Data storage and security

The Huntington's Disease Association has clear procedures in place to ensure the safe storage of personal data.

When processing confidential and personal information of supporters, members, volunteers and those who access our services, we will ensure that this information is recorded and stored securely within the relevant charity database or information storage system e.g. password protected excel spreadsheet.

Where Branches and Support Groups hold personal information, it will be stored securely. When held on computers, the computers will be password protected with up to date software to protect them from malware and viruses. Where information is stored on paper it will be filed securely. Groups will minimise the places they are storing data ideally with one central list of contacts which one person looks after. In branches, this would normally be the Secretary.

Where confidential and personal information is stored electronically by staff, it will be stored on a secure server with password protection / encryption in place with access

details shared only with those authorised to view the information. This removes the need for storage of personal information on individual electronic devices. Restricted access and permissions will be applied within our secure server to restrict and prevent unauthorised disclosure where relevant.

In cases where the Huntington's Disease Association is unable to store personal information on the relevant charity database or information storage system, it will be stored in a paper format. Where paper records are required, this information will be kept in a locked filing cabinet or drawer.

All electronic devices including computers, laptops and mobile phones will be password protected to ensure that confidential and personal information is stored both safely and securely without risk of unauthorised disclosure or loss. Computer, database and server passwords should be as a minimum eight characters long including at least one capital letter, one symbol and one number. Where available, two factor authentication should be implemented. Passwords to access the charity's secure server must be changed periodically when prompted.

All charity provided mobile phones will have a six-digit password and where practical all personal and confidential information stored on these devices will be stored in a minimised and time-limited format.

Public Wi-Fi must not be used as unsecured Wi-Fi connection makes it easier for hackers to access private files and information, and it allows strangers to use your internet connection.

Archiving, removal and destruction

All personal and confidential information will be stored until it is no longer required or until such time as it has fulfilled the original purpose for which it was collected and processed. Where personal information is no longer required or it is out of date it will be destroyed at the earliest possible opportunity.

When a service user has died or there has been no contact for three years and there is a paper file in existence the paper file will be sent to the Operations Team for archiving (clearly marked with an archive slip for each file) for destruction in six years from date of last contact. Any electronic records in existence will be marked as 'archived' on filemaker after three years of no contact or after the person has died. They will be deleted or stripped of confidential information after six years from date of last contact.

When a supporter has died or there has been no contact for six years, any electronic records that include financial transactions must be kept for six years until they can be destroyed. Notification will also be added to the database to ensure that the file is updated accordingly to remove data that is no longer required and to prevent contact in the future.

A register of voting members, including name, date membership commenced and voting number will be kept indefinitely whilst the charity is in existence. Where a voting member is deceased, information will be updated to ensure correspondence ceases but a record of their membership will be retained.

An annual review of all files will be undertaken to ensure that personal and confidential information is not stored and processed for longer than is required to fulfil the purpose for which it was collected.

The information management policy should be read in conjunction with this policy for full details of agreed charity retention periods.

Information sharing

We take the security and confidentiality of the personal information provided to us very seriously and we will only share information with other individuals, agencies or organisations where permission has been given. However, we may share personal information with the police and other agencies if we have concerns about the person or someone else if:

- We believe that the person's life or someone else's life is in danger.
- We are informed that a person or someone else is at risk of harm.
- Where it is necessary to share personal information for the purposes of safeguarding the interests of children and adults at risk.
- It is necessary to share the personal information to prevent or detect a crime.
- We are required to share the information under a Court Order or other regulation or legislation.

When there is a duty to share confidential information for legislative or reasons of regulations, special attention will be paid to ensuring that the information shared is complete, accurate, up-to-date and fit for purpose.

Where information is shared with other individuals, agencies or organisations, the information shared will be restricted to the subject matter for sharing and information minimised to fulfil the requirement of the initial sharing request. The information will be shared on a need to know basis and the recipients will only receive information that is relevant to the case.

Relatives, next of kin, carers or significant others will only have access to a service user's records where permission has been given by the service user or there is an appropriate lasting power of attorney in place.

Unique Reference Numbers (URNs) are available through the Huntington's Disease Association's databases and will be used at all times when sharing information about individuals internally. This ensures individuals can only be identified by those with access and permissions to view the respective management systems.

When personal and confidential information is shared, either internally or externally, special attention is given to ensuring that the information is sent to the intended recipient to prevent unauthorised or unintended disclosure.

Personal information shared electronically will be password protected or encrypted. The passwords needed to access the personal information will be shared via an alternative delivery method as an added security measure.

Where personal information is shared electronically with the Huntington's Disease Association by other organisations and third parties, we will implement and continuously comply with their secure email service settings to prevent loss or unauthorised disclosure of personal information.

We have a duty to safeguard and protect the interests of children who access our services. Communication will only be undertaken where permission has been granted by the parent, guardian or carer of the child. We adopt the following approaches in communicating with children and young people:

- We ensure that all information is communicated using the appropriate language, avoiding the use of words, phrases and jargon which has the potential to be misinterpreted.
- Where images are being sent and shared we will ensure that the images are age appropriate.
- Where electronic information is being shared with children and young people we ensure that this information is appropriate to the recipient.
- Where web information and hyperlinks are being shared with children and young people we ensure that the content is appropriate.

Subject access request

Right of access

The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data as well as other supplementary information. It helps individuals to understand how and why the Huntington's Disease Association is using their data, and check it is lawful. Individuals have the right to obtain the following:

- confirmation that the Huntington's Disease Association is processing their personal data
- a copy of their personal data, and
- other supplementary information – this is the information provided in a privacy notice

In addition to a copy of their personal data, the following information should also be confirmed:

- the purposes of processing information
- the categories of personal data concerned
- the retention period for storing the personal data
- the existence of their right to request rectification, erasure or restriction or to object to such processing
- the right to lodge a complaint with the Information Commissioners Office (ICO)
- information about the source of the data, where it was not obtained directly from the individual
- the existence of automated decision-making (including profiling)

In the event that the subject access request relates to a child, even if the child is too young to understand the implications of subject access rights, it is still the right of the child rather than of anyone else, such as a parent or guardian, to make a subject access request. Where relevant, the charity will respond directly to the child, unless the child authorises the parent or guardian to act on their behalf, or if it is evident that it is in the best interests of the child to liaise directly with their parent or guardian. The following will be taken into account when deciding whom to liaise with in relation to the Subject Access Request:

- the child's level of maturity and their ability to make decisions like this
- the nature of the personal data
- any court orders relating to parental access or responsibility that may apply
- any duty of confidence owed to the child or young person
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment
- any detriment to the child or young person if individuals with parental responsibility cannot access this information, and
- any views the child or young person has on whether their parents should have access to information about them

Subject access request procedure

Individuals can make a subject access request via telephone to 0151 331 5444, email info@hda.org.uk or in writing to Huntington's Disease Association at Suite 24, Liverpool Science Park, IC1, 131 Mount Pleasant, Liverpool, L3 5TF.

An individual is only entitled to request their own personal data, and not to information relating to other people unless the information is also about them or they are formally acting on behalf of someone else and are able provide evidence of this entitlement for example, written authority to make to request or a relevant power of attorney. If there are doubts about the identity of the person making the request, the charity can ask for more information in order to confirm who they are. The period for responding to the request begins on the day the request is received.

The Huntington's Disease Association will respond to a request within a calendar month and a fee will not be charged to deal with a request in most circumstances. Where the request is manifestly unfounded or excessive, the charity may charge a "reasonable fee" for the administrative costs of complying with the request. A charge may also be made if an individual requests further copies of their data. If a fee is to be charged the individual will be informed and the charity will not comply with the request until the fee has been received.

The charity has the right to extend the time to respond by a further two months if the request is complex or a number of requests have been received from that individual. In such cases, the charity will inform the individual within a calendar month of receiving their request and explain why the extension is necessary.

Refusing to comply with a subject access request

The Data Protection Act 2018 states that complying with a request is not binding if it would mean disclosing information about another individual who can be identified from that information, except if:

- the other individual has consented to the disclosure or
- it is reasonable to comply with the request without that individual's consent

The Huntington's Disease Association can also refuse to comply with a subject access request if it is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature. Any information about an individual who is not the person making the Subject Access Request will be redacted.

If a decision is made by the Huntington's Disease Association to refuse to comply with a subject access request, the individual will be informed without undue delay and within a calendar month of receipt of the request. The individual will be informed of the reasons the charity is not taking action, their right to make a complaint to the Information Commissioners Office (ICO) and their ability to seek to enforce this right through a judicial remedy.

Record correction or deletion request

All service users, supporters, volunteers, members and employees are entitled to see all the personal information that the Huntington's Disease Association holds about them and correct any errors or omissions or request deletion of their data.

Right to rectification

Under data protection legislation, individuals have the right to have inaccurate personal data rectified and / or to have incomplete personal data completed.

When a request for rectification is received, the Huntington's Disease Association will take reasonable steps to ensure that the new data provided is accurate and will rectify the data if necessary.

Right to erasure

Individuals have the right to have their personal data erased if:

- the personal data is no longer necessary for the purpose it was originally collected or processed it for;
- consent is relied on as the lawful basis for holding the data, and the individual withdraws their consent;
- legitimate interests is relied on as the basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- the personal data is processed for direct marketing purposes and the individual objects to that processing;
- the personal data is processed unlawfully
- there is a requirement in order to comply with a legal obligation; or
- If the data being processed relates to the offer of information society services to a child.

There are circumstances in which the right to erasure does not apply, which includes

- compliance with a legal obligation
- for a task carried out in the public interest or in the exercise of official authority,
- for archiving purposes in the public interest, scientific research, historical research or statistical purposes where erasure would impair the achievement of the processing
- For the establishment, exercise or defence of legal claims
- To exercise the right of freedom of expression and information

Data correction or deletion request procedure

All requests for the correction and / or removal of data should be either made via telephone to 0151 331 5444, email info@hda.org.uk or in writing to Huntington's Disease Association at Suite 24, Liverpool Science Park, IC1, 131 Mount Pleasant, Liverpool, L3 5TF.

We will respond and action all requests for information to be altered, corrected or removed within one month of receipt of the request. Where a request for correction or deletion is received, no charge will be levied for undertaking such a request.

It is the responsibility of all staff to ensure that such requests are dealt with effectively, within required timescales and that reasonable steps have been undertaken to ensure that the request is valid and meets the relevant criteria for deletion or rectification. The Huntington's Disease Association will regularly review and monitor performance to ensure ongoing compliance.

Where the Huntington's Disease Association has verified that the original data is accurate and should not be rectified or that data does not meet the criteria for erasure, the individual will be informed of the decision not to take further action. They will also be informed of their right to make a complaint to the ICO or another supervisory authority and their right to seek to enforce this right through a judicial remedy. In such cases, a note will be made on the relevant system to indicate that the individual has either challenged the accuracy of the data or has requested that the data be erased and the reasons why the charity has chosen not to meet their request.

Data processing objection

Right to object

Under GDPR, individuals have the right to object to the processing of their personal data in certain circumstances. This is an absolute right to stop data being used for direct marketing, whereas in other cases, a request must be made submitting a compelling reason for consideration.

Objection to processing procedure

All objections to the processing of personal data should be made verbally by telephone to 0151 331 544 or in writing to info@hda.org.uk or to Huntington's Disease Association at Suite 24, Liverpool Science Park, IC1, 131 Mount Pleasant, Liverpool, L3 5TF. Where this relates to direct marketing, an opt-out link may be used which will prompt an automated change to how data is processed to comply with the individual's wishes.

We will respond and action all objection requests within one month of receipt of the request. Unless it relates to direct marketing, in which case this will be actioned immediately on receipt. Where an objection request is received, no charge will be levied.

Data breaches

What is a data breach?

A data breach is any failure pertaining to personal information and data that does not meet the requirements of data protection legislation. A data breach can include unlawful or unauthorised disclosure or use of personal information, the recording or sharing of inaccurate personal information and the unlawful processing of personal information. Breaches can be the result of both accidental and deliberate causes. Personal data breaches can include:

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a controller or processor
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data

Data breach expectations

As part of our commitment to safe and secure processing of personal information, we will ensure:

- All staff and volunteers are able to recognise a personal data breach.
- All staff and volunteers are clear and understand how to report data breaches.
- Those responsible for the management of personal data breaches within their service area are aware of where to log the breach and the action that must be taken depending on the gravity through consultation with the Data Protection lead.

Data breach assessment and reporting

Data breaches should be discussed with the charity's Data Protection lead and reported within 72 hours of discovery to the Information Commissioner's Office where the relevant criteria is met. If the breach has a high risk of adversely affecting people's rights and freedoms, the Huntington's Disease Association will inform those individuals of the relevant details of the breach without undue delay including:

- the nature of the personal data breach
- the name and contact details of the Data Protection lead or other contact point where more information can be obtained
- a description of the likely consequences of the personal data breach
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects

The Data Protection Lead will notify the Information Commissioner's Office (ICO) if the breach is severe enough to pose a risk to the individual's rights and freedoms. If a decision is made not to report, the decision should be justified and documented. The charity will keep a record of any personal data breaches, regardless of whether it is required to notify the individual or ICO. The ICO has an online self-assessment that the Data Protection Lead will use to help determine whether the breach needs to be reported to the ICO.

The charity will also consider the need to notify third parties, such as the police, insurers, professional bodies, or bank or credit card companies who may be able to help reduce the risk of financial loss to individuals dependent on the nature of the breach.

In assessing risk to rights and freedoms, the Huntington's Disease Association will focus on the potential negative consequences for individuals. When reporting a breach the following information needs to be included:

- the categories and approximate number of individuals concerned
- the categories and approximate number of personal data records concerned

- the name and contact details of the data protection lead or other contact point where more information can be obtained
- a description of the likely consequences of the personal data breach
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects

Where a significant cyber incident occurs, the Huntington's Disease Association may also need to report this to the National Cyber Security Centre (the NCSC) depending on the nature of the breach.

Where a data breach might lead to a heightened risk of individuals being affected by fraud, the Huntington's Disease Association should report the incident to Action Fraud – the UK's national fraud and cybercrime reporting centre.

Data Protection Impact Assessment

What is a Data Protection Impact Assessment (DPIA)?

A DPIA is a way for the charity to comprehensively analyse our data processing and help identify and minimize data protection risks. DPIAs are a legal requirement for processing data that is likely to be high risk.

DPIAs should consider compliance risks (Legal compliance such as data protection legislation and PECR and organisational compliance such as policies and procedures), but also broader risks to the rights and freedoms of individuals. The focus is on the potential for harm, to individuals or to the wider society. To appropriately assess the level of risk, the assessment should consider both the likelihood and the severity of any processing and its impact on the individuals involved. A DPIA does not have to eradicate risk altogether, but it should identify measures to minimize risks and assess whether any remaining risk can be justified.

When should a Data Protection Impact Assessment (DPIA) be carried out?

The Huntington's Disease Association should carry out a DPIA, using the agreed charity template form, before beginning any type of data processing that is likely to result in a high risk in order to minimize the data protection risks of a project. This could be a new project or if changes are planned to an existing project. In order to determine whether a DPIA needs to be completed, the Information Commissioner's Office (ICO) has produced a checklist to help determine situations in which a DPIA should be considered or is required.

The ICO recommend that a DPIA should be considered if any of the following are planned as part of a new project, or an existing project that is subject to change, that will involve the use of personal data:

- evaluation or scoring;

- automated decision-making with significant effects;
- systematic monitoring;
- processing of sensitive data or data of a highly personal nature;
- processing on a large scale;
- processing of data concerning vulnerable data subjects;
- innovative technological or organisational solutions;
- processing that involves preventing data subjects from exercising a right or using a service or contract.

The ICO recommend that a DPIA should always be undertaken if any of the following are planned as part of a new project, or an existing project that is subject to change, that will involve the use of personal data:

- use systematic and extensive profiling or automated decision-making to make significant decisions about people;
- process special-category data or criminal-offence data on a large scale;
- systematically monitor a publicly accessible place on a large scale;
- use innovative technology in a manner that could threaten an individual's privacy;
- use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit;
- carry out profiling on a large scale;
- process biometric or genetic data;
- combine, compare or match data from multiple sources;
- process personal data without providing a privacy notice directly to the individual;
- process personal data in a way that involves tracking individuals' online or offline location or behaviour;
- process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them;
- process personal data that could result in a risk of physical harm in the event of a security breach.
- there is a change to the nature, scope, context or purposes of our processing.

If The Huntington's Disease Association decides not to carry out a DPIA, the reasons why this course of action has been chosen should be documented.

The Huntington's Disease Association may also consider it relevant to complete a DPIA following a security incident or breach, where a concern has been raised or where risks have been identified that require appropriate management.

If there is uncertainty regarding whether it is appropriate to carry out a DPIA for a specific project, by default employees should proceed cautiously and complete a DPIA. The charity's Data Protection Lead can also be consulted for clarification and further guidance.

All completed DPIA's should be completed and sent to the Data Protection Lead before any project progress is made for their authorization and / or further recommendations.

If a DPIA indicates that the data processing is high risk and these risks cannot be sufficiently addressed, the ICO should be consulted for an opinion on whether planned date processing complies with data protection legislation.

On completion of the DPIA, the results and agreed actions identified to reduce risk factors should be included in the relevant project plan.

The Information Commissioner's Office (ICO)

The Information Commissioner's Office is the supervisory authority for data protection in the United Kingdom. They are able to provide information and advice and they are responsible for the investigation and sanction of any potential breaches of the legislation. The Huntington's Disease Association will make contact with the ICO as required.

Key contacts

Data Protection Lead	John Gandy Phone: 07900922529 Email: john.gandy@hda.org.uk
Information Commissioner's Office (ICO)	Website: www.ico.org.uk
National Cyber Security Centre (the NCSC)	Website: www.ncsc.gov.uk
Action Fraud	Website: www.actionfraud.police.uk