YMCA DERBYSHIRE

Data Protection Policy

Approved by the Board: 25 June 2020
Review Date: June 2022
Version: 6

Contents

Definitions:

Data Controller	The individual or the legal person who controls and is responsible for the keeping and use of personal information on computer or in structured manual files.
DPA	Data Protection Act 2018
Data Protection Officer	The postholder within an organisation who acts as an independent advocate for the proper care and use of individual information.
Data subject	Any individual person who can be identified, directly or indirectly, via an identifier such as a name, an ID number, location, data, or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity.
EU	European Union
GDPR	General Data Protection Regulation
ICO	Information Commissioner's Office
Personal Data	Data that relates to an identified or identifiable individual and is: • processed electronically • kept in a filing system • part of an accessible record, for example an education record held by a public authority This includes data that does not name an individual but could potentially identify them.
Privacy Notice	A privacy notice states what to expect from an organisation with regard to an individual's personal information when they make contact with the organisation or use the organisation's services.
Subject Access Data Request	A request sent from a data subject to a Data Controller requesting information about themselves. (It is a legal requirement under the Data Protection Act (DPA) for the data controller to comply with this request normally within a month timescale as outlined in the DPA).
Unlawful processing	If no lawful basis applies to the processing of data, it will be unlawful. Individuals have the right to request the erasure of personal data which has been processed unlawfully.

Data Protection Policy

1. Policy Statement

The Data Protection Act 2018 controls how personal information is used by organisations, businesses and the government.

The Data Protection Act 2018 is the UK's implementation of the GDPR.

Both employers and employees have new responsibilities to consider to help ensure compliance.

YMCA Derbyshire ("the Association") must ensure that all personal information collected by the organisation is used appropriately, stored securely, shared responsibly and destroyed correctly when the information is no longer required. The Association's priority is to comply with the legislation and the requirements of the ICO.

This policy does not form part of any employee's contract of employment and it may be amended at any time.

2. Scope

This Data Protection Policy applies to all of the Association's trustees, staff, volunteers and contractors (known as the Association's personnel) who collect, store, handle, amend, use, share, view and/or destroy 'personal data' in the course of their role and responsibilities.

This policy demonstrates that the Association will:

- Be open about the reasons why there is a need to collect personal information;
- Ensure that we only collect the personal information we need and do not keep it for longer than necessary;
- Ensure the data we hold is adequate, relevant and limited to what is necessary in relation to the purpose(s) for which is it processed;
- Accurate and where necessary, kept up to date;
- Processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3. Definition of Personal Data

Personal data is any information relating to an identified or identifiable individual (defined as a 'data subject' under the data protection legislation). This includes information which would identify the individuals if linked to other information we hold. For example, if we use a case reference number, we can still identify the individual because we have a link that shows the individual's name and their case reference number.

Information about an organisation is not subject to the data protection legislation. So information about the Association, for example, is exempt until it has an individual's name linked to it.

In the context of the Association this would include, for example, the names, addresses and other information relating to employees, trustees, volunteers, supporters, clients, anyone who corresponds with us, applicants for housing, education or our family services, residents, students, donors, information about named individuals contained in our files, computer systems or other records, etc.

4. Role of Data Protection Officer

The role of Data Protection Officer at the Association will be shared between the Director of Finance, Andrew Armstrong and the Director of HR, Jane Lunn. The role will be to:

- Inform and advise the organisation and our employees about our obligations to comply with data protection laws;
- Monitor compliance with data protection laws, including the management of internal data protection activities, arranging staff training and conducting internal audits;
- Be the first point of contact for individuals whose data is processed (employees, customers, etc);
- Ensure relevant documentation is compliant with the legislation;
- Report on a regular basis to the Senior Leadership Team and to the Board.

5. Definition of Information

Information is any record whether in computerised format or a highly structured paper filing system. This can include text messages, letters, post-it notes attached to a file, emails, record sheets, file notes, etc.

6. Policy Statements

i. All personal data will be protected by data protection mechanisms to ensure the highest levels of confidentiality, integrity and availability.

ii. Only personnel that have previously been authorised are allowed to enter personal data into an information system. Inputs will be restricted according to granted permissions, though these restrictions may be lifted on a temporary basis for legitimate pre-defined operational reasons. In such circumstances, additional authorisation is required and must be granted before restrictions are lifted.

iii. Where possible, information systems will check entered personal data for accuracy, completeness, validity and authenticity. These checks will be performed as close to the point of entry as possible to ensure that corruption does not occur.

iv. Information systems will be configured such that they prevent unauthorised and unintended information transfer. Further, information systems will protect the integrity and confidentiality of transmitted personal data using data encryption methods.

7. What to Consider when Collecting Personal Data

The data protection legislation governs the 'processing' of personal data by the Association. This covers any operation performed on personal data, including collecting, storing, consulting, using, referencing, disclosing, amending or deleting.

The Association's personnel must comply with the following principles to ensure that any personal data processed is:

i. Processed lawfully, fairly and in a transparent manner in relation to individuals. Personal data must only be processed where there is a legal basis under the data protection legislation and individuals must be told what we are using their personal data for and why;

ii. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. We will only use an individual's personal data for the purpose it was collected;

iii. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. We will only ask for personal data that is needed for a legitimate purpose (i.e. a person will not be asked for their life history when all that is needed is their name and address);

iv. Accurate and, where necessary, kept up to date. We will take steps to delete or correct personal data that is inaccurate, having regard to the purposes for which it is processed, without delay;

v. Kept in a form that identifies individuals for no longer than is necessary for the purposes for which it is proposed. We will only keep personal data for as long as we need it; and

vi. Processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. The Association will ensure that personal data is kept secure in accordance with our policies.

When processing personal data the Association's personnel will be responsible for the general duty of care and confidentiality owed to individuals when dealing with their personal data. This means, for example, ensuring that:

- where it may not be obvious, it is made clear to individuals why they are being asked for information, how it will be used and who it will be shared with; and
- personal data is treated with respect in both terms of what is done with it and who we disclose it to; and
- we do not express a subjective opinion about an individual which cannot be substantiated by the facts.

This applies to all the personal data held by the Association, whether it is stored electronically or in structured manual filing systems.

8. Ensuring Compliance when Processing Personal Data

When we process personal data, we must meet at least one of the following conditions:

- The individual has given their consent to us for their personal data to be processed. This is most easily carried out at the point we collect it. For example, we notify someone who is completing a form what the personal data will be used for, how it will be stored and who it will be shared with. There are limited circumstances where we can ask for consent under data protection legislation;

- The personal data is necessary to perform a contract between the Association and the individual or to take steps to enter into such a contract. For example, the personal data is necessary in order to ascertain an applicant's eligibility for a residency or to send out information regarding a training and education course or details about our wraparound care;

- The personal data is required to comply with a legal obligation to which the Association is subject. For example, the Association is required to process employees' personal data for PAYE and National Insurance obligations;

- The personal data is necessary in order to protect the vital interests of the individual. This only applies for matters of life and death. For example, the disclosure of an individual's name and date of birth to a hospital casualty department treating them; or

- The processing of the personal data is necessary to pursue the Association's or a third party's legitimate interests. This only applies where the Association's or a third party's legitimate interests are not overridden by the interests, rights or freedoms of the individual.

9. Special Categories of Personal Data

Where information relates to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership or involves genetic, biometric data, data concerning health or an individual's sex life or sexual orientation, this is known as "special categories of personal data".

The Association may only process special categories of personal data where one of the following applies:

- The individual has given their explicit consent for us to process their personal data;

- The personal data is required for the Association to comply with obligations under employment, social security or social protection law. For example, the requirement to maintain employees' absence records as an employer;

- The personal data is necessary in order to protect the vital interests of the individual. This only applies for matters of life and death. For example, the disclosure of an individual's medical history to a casualty department treating them;

- The processing relates to personal data that has manifestly been made public by the individual;

- The personal data is required to establish, exercise or defend legal claims. For example, the Association needs to refer to or rely on personal data in order to defend an action raised against the organisation in court;

- The processing of the personal data is necessary for reasons of substantial public interest under law. For example, to prevent or detect unlawful acts by disclosing personal data to the police; or

- The processing of the personal data is necessary for health or social care purposes. For example, to assess the working capacity of an employee or provide social care.

The Association must take particular care when processing and storing special categories of personal data to ensure that it is held securely. Lots of the information held by the Association about residents, learners and children comprises special categories of personal data. These records should therefore be held securely and access restricted to those who need to see the records.

10. The Impact of Data Protection on Day to Day Work

10.1 Asking for personal data in letters, emails or by telephone

When asking someone for personal data, such as their name and address, we must provide them with a Privacy Notice either at the time or as soon as possible afterwards and which explains:

- The identity and contact details of the Association and our Data Protection Officer;

- The purpose and legal basis for processing their personal data;

- If we are processing their personal data to pursue legitimate interests, we need to explain what those are;

- Details of any recipients of their personal data, including whether their personal data is transferred outside the EU and what safeguards the Association has put in place for the transfer;

- How long the Association will keep their personal data or the criteria used to determine this;

- Details of each of the individual's rights under the data protection legislation;

- Information on the individual's right to complain to the ICO; and

- Whether the personal data is required for a statutory or contractual requirement and the reasons for requesting that data.

The Association does not currently use any automated decision-making for the personal data that is processed. If this changes, however, the Privacy Notice should also include details of this.

It is important when asking an individual for their personal data that we provide them with a Privacy Notice setting out the information above and:

- Only asking for information that is really needed;
- Explaining why the information is needed and what it is intended to be used for (if it is not obvious);
- If the information will be published in some other way which will be open to public scrutiny (such as accounts and annual reports) then the individual should be told so;
- If we want the information to pass on to someone else then we must explain who we intend to disclose it to and why and ask the individual if they object; and
- Do not imply that the person must provide the information if in fact they are under no legal obligation to provide it.

10.2 Receiving or recording personal data (including expressions of opinion)

Often, during the course of our work, personal data is received, sometimes in response to a direct request from us for the personal data, sometimes it is unsolicited. Sometimes this includes details of opinions expressed by ourselves or others about particular individuals, which are recorded in letters, emails or internal minutes or in the write up of a phone call, interview or visit.

Where we have been provided with personal data and we need to retain it, it should be recorded and stored appropriately. We must also consider whether we need to provide the individual with a Privacy Notice if they did not provide their own personal data to us. Such a Privacy Notice needs to include the information listed in paragraph 10.1 above, together with a list of the categories of personal data received and who we received it from.

We must provide individuals with a Privacy Notice as soon as possible after receiving an individual's personal data from a third party, unless they already have the information contained in the Privacy Notice or providing them with a Privacy Notice would involve a disproportionate effort.

11. Using Personal Data

When using personal data:

- It should only be used for the purposes for which it has been obtained;
- You should only keep it for as long as you need it (i.e. do not keep it indefinitely on the off chance that it might come in useful one day) and destroy it when you no longer

have a use for it or in accordance with the Associ ation's Data Retention Policy and schedules;

- Take reasonable steps to make sure that it is accurate and up to date. This applies to personal data for which we have a continuing use. It does not mean, for example, that we must continue to update addresses for people with whom we have corresponded in the past. If we are unlikely to contact them again, then we do not have to maintain that information. However, if we need to maintain an accurate and up to date correspondence address, then we must take steps to ensure its accuracy and relevance; and

- Do not disclose any personal data to anyone outside the Association, unless we have told the individual concerned in advance that their personal data would be disclosed to that recipient within a Privacy Notice or have obtained the consent of the individual (if appropriate).

12. Storing Personal Data

All records, whether electronic or paper or whether or not they contain personal data, must be stored securely. This includes, for example:

- Storing paper records in an appropriate file and electronic records in an appropriate directory;

- Retaining records in good order so that they can be clearly identified and retrieved;

- Retaining records for an appropriate length of time in accordance with our Data Retention Policy and schedules; and

- Ensuring the appropriate destruction of records when we no longer have a legitimate use for the information. Records should be destroyed in accordance with our Data Retention Policy and schedules.

13. Disclosing Information in Relation to Legal Proceedings

There may be circumstances in which it is necessary to disclose personal data in relation to legal proceedings. Obviously in such cases it will be necessary to disclose personal data to someone other than the individual. If you are asked for information about an individual you should check with the Data Protection Officer before providing it.

14. Paper Records

The Data protection legislation captures certain personal data which is held in paper files. This personal data is usually organised in such a way that specific information relating to a particular individual be can easily found.

The Association has a variety of paper records across each of its departments and some of these are structured so that information regarding a given individual could be easily retrieved. Where this is the case, we will handle these records in accordance with the Data protection legislation in the same way as electronic records.

Although there are exemptions to the right of access by individuals, as a general rule, it would be wise to assume that if we hold personal data, even in paper form, this would fall within the scope of a subject access request and the individual is likely to have right of access to it under the provisions of the Data protection legislation.

15. Allowing Access to our Records

The Data protection legislation allows individuals to request access to their personal data held by organisations and this is known as the right of subject access.

15.1 Who deals with requests?

All subject access requests must be made in writing (which should include requests made by email). In the case of access to HR records, requests for access should be dealt with by the Director of HR. In all other cases written requests should in the first instance be forwarded to the Director of Finance.

If someone telephones or visits any of our premises requesting access to their personal data, they should be asked to submit their request in writing or by email to the Director of Finance.

All written requests must be date stamped on receipt.

Requests will be dealt with by a person nominated by the Director of Finance, and they will need to consult other members of staff who may be holding the personal data requested or in order to determine what information falls within the scope of the request.

It is important that all of the Association's personnel understand what is involved in this process and we must co-operate to ensure that we are able to meet the deadline for responding to such requests, which is normally within one month from the date of receipt. It is also vital that we maintain our records in good order so that this information may be retrieved as quickly and efficiently as possible.

The nominated officer will then identify whether the request is valid or not. The nominated officer may need to ask the requestor for further information before they are able to respond to the request.

15.2 Deciding what personal data may be released

On receiving a written subject access request, the nominated officer must:

- Contact the Director of Finance or the Director of HR who both act as the Data Protection Officer, to obtain advice;
- Ensure that the person making the request is the individual about whom the personal data relates (or if not, do they meet the criteria to apply on someone else's behalf);
- Establish the extent of the personal data they are requesting;

- Ensure that disclosure of the personal data requested will not disclose a third party's personal data (unless the third party consents or it is reasonable to dispense with their consent);

- Consider whether it would take a disproportionate effort to provide the personal data requested (i.e. is the information requested reasonably easy to provide within the timescale); and

- Determine whether the requester has made a previous similar request and, if so, whether a reasonable time interval has lapsed between the request and the current request.

15.3 Releasing personal data

In order to request the personal data, the nominated officer shall:

- Consider the terms of the subject access request to identify the scope of the information requested;

- Search through the Association's records to locate the personal data relating to the requestor using simple terms such as 'John' or 'Smith' and/or other nicknames or acronyms by which the requestor may be known within the Association, such as "AB";

- Once all of the information has been located and collated the nominated officer shall review the information to determine what falls to be disclosed in response to the relevant subject access request. The requestor's personal data is any piece of information which has the requestor as its focus – i.e. they are the subject of that information. Any incidental reference to the requestor within a document, letter or email would not be enough in and of itself to render that document, letter or email the requestor's personal data; and

- Following identification of all of the requestor's personal data falling within the scope of their subject access request, the nominated officer shall consider whether any information is exempt and must be redacted or withheld. For example, third party personal data.

  The requester should be provided with all the personal data relating to them which meets their subject access request (provided that this does not involve disproportionate effort), that is not exempt and will not disclose personal data relating to another individual (without first obtaining their consent).

  Any response to a subject access request must also provide the requestor with information on how we use their personal data. This means that we need to include the information that is required in a Privacy Notice to the requestor in response to their request.

15.4 Refusing to release personal data

We should refuse to supply the information where:

- We are not satisfied that the requester is the individual concerned (or their appointed representative);
- The subject information rights under the Data protection legislation do not apply;
- All the information requested is exempt; or
- Meeting the request involves disproportionate effort.

In responding to the request, the nominated officer will set out clearly the reasons for the refusal, such as any specific exemptions that apply, and any additional information which is thought will help the requestor to understand the reason for refusal. The requestor will also be advised of the right to make a complaint to the ICO and their ability to seek to enforce this right through a judicial remedy.

We should not refuse to deal with a request on the basis that some of the personal data is exempt. In such cases we should provide the personal data that is not exempt and clearly explain why other personal data requested cannot be supplied.

15.5 Responding to Manifestly Unfounded or Excessive Requests

A request may be manifestly unfounded if the individual has no clear intention to access the information or is malicious in intent and is using the request to harass the Association with no real purposes other than to cause disruption.

Factors that may indicate malicious intent include:

- the requestor has explicitly stated, in the request itself or in other communications, that they intend to cause disruption;
- the request makes unsubstantiated accusations against the Association or specific employees;
- the individual is targeting a particular employee against whom they have a personal grudge; or
- the individual is systematically or frequently sending different requests as part of a campaign with the intention of causing disruption, e.g. once a week.

These factors will not automatically mean a request is manifestly unfounded, and we will consider any request within the context in which it is made.

A request may be excessive if it:

- repeats the substance of previous requests and a reasonable interval has not elapsed; or
- overlaps with other requests.

We will handle all requests on a case by case basis. A request may not be excessive just because the requestor has asked for a large amount of information. The Association can ask for more information to help locate the information they want to receive.

Where a requestor may also want to receive another copy of information they have requested previously, the Association can charge a reasonable fee for the administrative costs of providing this information again and it is unlikely that this is an excessive request.

In deciding whether a reasonable interval has elapsed between requests the Association will consider:

- the nature of the data – this could include whether it is particularly sensitive, but also the value of the information to the individual;
- the purposes of the processing – these could include whether the processing is likely to cause harm to the requester if disclosed;
- how often the data is altered – if information is unlikely to have changed between requests, it could be considered not to respond to the same request twice.

15.6 Charging a Fee

Under Part 3 of the DPA 2018, we can no longer request a fee for processing a subject access request. However, we may charge a reasonable fee where we decide that a request to exercise a right under sections 45, 46, 47 or 50 is manifestly unfounded or excessive, but we still choose to respond to it.

If we do decide to charge a reasonable fee, we will need to justify the cost and notify the requester and say why. We will not need to send the information or respond to the request until we have received the fee. The time limit for sending our response to the request will then begin once the requester has paid the fee.

15.7 Timescales for dealing with Subject Access Data Requests

We must comply with a request promptly and in any event within one month of receipt of a valid request.

Where the request is such that it cannot be dealt with promptly, we should contact the requestor acknowledging their request and explaining reasons for the delay. We may be able to extend the time period for responding to any complex and numerous requests by two months. This time period is set out in the Data protection legislation and must be complied with.

16. Right to Rectification

The right to rectification gives individuals a right to have their personal data corrected if it is inaccurate or incomplete. When the Association receives a request from an individual to rectify their personal data, we have one month to respond (this can be extended by two months for complex requests).

If the Association complies with this request, any third parties who have received the relevant personal data must be informed of the rectification if possible and details of any such third parties must be given to the individual.

If the Association decides not to take action in response to a request for rectification, we must explain why to the individual and let them know that they can complain to the ICO or seek a remedy through the courts.

Any requests for rectification must be provided to the Data Protection Officer immediately upon receipt, together with a copy of the relevant personal data and any comments relating to its accuracy.

Most requests to update their personal data, for example, where a resident or learner provides the Association with updated contact details, will be able to be dealt with on a day to day basis. However, any official requests that reference the Data protection legislation, contain extensive amendments, or relate to personal data that the Association feels is accurate, should be passed to the Director or Finance or Director of HR to respond to.

17. Right to Erasure

The right to erasure is also know as the 'right to be forgotten' and allows an individual to request that the Association deletes or removes their personal data where there is no compelling reason to continue processing it.

This right applies in the following circumstances:

- Where the personal data is no longer necessary for the purpose it was originally collected/processed;
- When the basis for processing the individual's personal data is consent and they withdraw their consent;
- When the individual objects to the processing of their personal data and the Association does not have an overriding legitimate interest to continue the processing;
- The personal data was unlawfully processed, i.e. in breach of the Data protection legislation;
- The personal data has to be deleted in order to comply with a legal obligation; and
- The personal data is processed in relation to targeting online services to a child.

The Data Protection Officer has responsibility for determining whether a request for erasure can be complied with. There are certain circumstances when the Association can refuse a request for erasure, such as when the personal data is processed for the following reasons:

- To exercise the right of freedom of expression and information;
- To comply with a legal obligation to perform a public interest task or exercise official authority;
- For public health purposes in the public interest;

- For archiving purposes in the public interest, scientific research, historical research or statistical purposes; or

- To establish, exercise or defend legal claims.

If the Association deletes any personal data following a request for erasure that has been disclosed to third parties, the Association must inform the third parties about the deletion, unless it is impossible or involves disproportionate effort to do so.

Any requests for erasure must be provided to the Data Protection Officer upon receipt, together with a copy of the relevant personal data and any comments relating to the reasons for processing it.

18. Right to Restrict Processing

The right to restrict processing allows individuals to request that the Association restricts the processing of their personal data. When processing is restricted, the Association can still store the individual's personal data but cannot process it any more.

The Association will need to restrict the processing of personal data in the following circumstances:

- When an individual claims that the personal data is inaccurate, the processing of that personal data should be restricted until the accuracy of it is verified;

- When the Association is considering if our legitimate interests override those of the individual where the individual has objected to the processing of their personal data;

- When the Association's processing is unlawful and the individual requests restriction of the processing of their personal data rather than erasure; and

- When the Association no longer needs the personal data but the individual requires their personal data to establish, exercise or defend a legal claim.

The Data Protection Officer is responsible for determining if any processing of personal data is to be restricted and any requests for restriction must be provided to the Data Protection Officer upon receipt, together with a copy of the relevant personal data and any information regarding the processing.

19. Right to Data Portability

The right to data portability allows individuals to obtain personal data from the Association and reuse it for their own purposes. For example, this could apply to an employee moving between employers.

This right only applies to personal data provided to the Association by an individual, where the Association processes the personal data based on the individual's consent or in order to perform a contract, and the processing is carried out by automated means (i.e. inputted into any of the Association's IT systems).

The Association has one month to respond to requests for data portability and the Data Protection Officer has responsibility for responding to these. Any requests for data portability must be passed to the Data Protection Officer immediately, together with a copy of the personal data requested by the individual.

20. Right to Object

An individual is entitled, by written notice, to require the Association to cease or not to commence using their personal data for the purposes of direct marketing. That is, providing them with advertising or marketing material. If we fail to remove their consent from our system, they may apply to the court for an order or ask the ICO to investigate on their behalf.

Individuals have the right to object to the Association's processing of their personal data where it is used for:

- Legitimate interests or to perform a task in the public interest/exercise of official authority:
  - individuals can object for reasons relating to their particular situation; and
  - the Association must stop processing the personal data unless our legitimate interests override those of the individual or the processing is to establish, exercise or defend legal claims;
- Direct marketing:
  - as soon as the Association receives an objection to direct marketing activities, we must stop processing the individual's personal data for direct marketing purposes immediately; and
- Scientific/historic research and statistics:
  - individuals can object for reasons relating to their particular situation; and
  - the Association is not required to comply with an objection where the processing of personal data is necessary for the performance of a public interest task.

The Data Protection Officer has responsibility for dealing with objections to processing and any objections to processing personal data must be passed to the Data Protection Officer immediately, together with a copy of the personal data details of the processing objected to.

21. Data Sharing

From time to time in the course of our work, we forward information about individuals to other organisations, such as the police, HMRC, other charities and similarly, they forward personal data to us. We need to ensure that we do not mislead individuals about the circumstances in which we might share data with other organisations. For example, if we require people to supply us with personal data on the understanding that it will remain confidential and, we then forward it to another organisation we may be in danger of breaching the Data protection legislation, particularly if that processing could not have been reasonably foreseen by the individual.

When we receive personal data from another organisation, we need to consider:

- The reliability of the source of that personal data;
- Why it has been provided to us;
- What we intend to do with the personal data;
- How long this personal data should be retained;
- What steps we will take to verify its accuracy; and
- At what point we should advise the individual concerned that it is in our possession.

Heads of Service and/or the Association's Data Protection Officer(s) should be notified when personal data is requested, before it is released or when information is received from other organisations.

22. Retention of Documents

Documents should be retained for the necessary period required by statute or good practice in accordance with our Data Retention Policy and schedules.

The Data Protection Officer can provide information, guidance and clarification regarding retention periods.

23. Destroying Personal Data

When personal data held is no longer required, the personal data should be destroyed using a secure method, for example, shredding, in accordance with the Data Retention Policy.

24. Responding to Mistakes

Where you have made a mistake, or you believe you may have made a mistake, you must contact the Data Protection Officer immediately. Whilst most data protection breaches may be minor, for serious data protection breaches we have an obligation to notify the ICO within 72 hours of the Association becoming aware of the breach. Further, where the breach puts individuals' personal data at risk (for example, unlawful disclosure of bank details) then we have to notify the individuals concerned immediately. Failure to notify a data protection breach to the ICO and/or individuals may result in the Association having to pay a large fine.

The responsibility for determining the seriousness of a data protection breach lies with the Data Protection Officer. Employees must report all breaches to the Data Protection Officer and not make a decision themselves on how serious a breach is. A record of breaches will be maintained and the circumstances reviewed to see how the breach could have been prevented. Ultimately, this may mean more training or a different process being put into place.

Examples of personal data protection breaches can include:

- access by an unauthorised member of staff or 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; and
- loss of availability of personal data.

25. Non-Compliance

Violations of this policy will be treated like other allegations of wrongdoing at the Association. Allegations of misconduct will be adjudicated in accordance with established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to the disciplinary policy and procedures;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual arrangements.

26. The Association's Personnel Responsibilities

The following of the Association's personnel will be required to read and operate within the contents of this Data Protection Policy:

- Employees
- Trustees
- Volunteers

This policy must be issued to contractors or other organisations where they either receive or send personal data from or to the Association.

27. Policy Review

The Association will review the content of this policy every two years or earlier in the event that there are changes in legislation or as a result of a change in good practice.

This policy links to:

Data Retention Policy and schedules
CCTV policy
Information Security Policy
Disciplinary Policy