.henshaws
beyond expectations

DP002 DATA PROTECTION POLICY

Review Date	Ratified Date	Next Planned Review
October 2025	February 2023	June 2026

Directorate (Indicate which applies by ticking the appropriate box)								
General	**Human Resources**	**Finance**	**College**	**ACC**	**Community Services**	**Health and Safety**	**Fundraising**	**Marketing**
x								

Version Number	Date	Reason for Change	Owner
1	March 2023	Introduction of new policy	Head of MIS
2	June 2024	Annual review	Head of MIS
3	June 2025	Annual review, change of roles, updated template from Judicium	Head of MIS
3.1	October 2025	References added to 3 new linked policies	Head of MIS

Author	**Head of MIS, based on Judicium Education template**
Ratified by	**HSMT**

Reason for this Review	Annual policy review
Were changes made?	Yes
Summary of changes	Annual review, change of roles, updated template from Judicium
Relevant Legislation	UK General Data Protection Regulation (UK GDPR)
Underpinning Knowledge – What have we used to ensure the policy is current	Documentation made available by Judicium Education (DPO), previous policy
Linked Henshaws Policies	• Data Breach Policy • Bring Your Own Device Policy • ICT Acceptable Use Policy • Remote Access Policy • Data Retention Policy • Record Keeping Policy • CCTV Policy • Henshaws AI Policy
Equality Impact Completed	See Appendix 3
Suggested Action	Disseminate to all staff, publish on the website

Aim and scope of policy

This policy applies to the processing of personal data in manual and electronic records kept by the Charity. It also covers the Charity's response to any data breach and other rights under the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018 and National Data Guardian's 10 Data Security Standards

The Charity makes a commitment to ensuring that personal data, including special categories of personal data and criminal offence data (where appropriate) is processed in line with UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018 and National Data Guardian's 10 Data Security Standards and domestic laws and all its employees conduct themselves in line with this, and other related policies. Where third parties process data on behalf of the Charity ("Processors"), the Charity will ensure that the third party takes such measures in order to maintain the Charity's commitment to protecting data. In line with GDPR UK, the Charity understands that it will be accountable for the processing, management and regulation, and storage and retention of all personal data held in the form of manual records and on computers.

Definitions

Personal data

Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.

Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.

Special Category Data and Data Relating to Criminal Convictions and Offences

Previously termed "Sensitive Personal Data", Special Category Data is similar by definition and refers to data concerning an individual Data Subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical and mental health, sexuality and biometric or genetic data.

Personal data relating to criminal offences and convictions is included here for the purposes of this policy. This refers to personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.

Data Subject

An individual about whom such information is stored is known as the Data Subject. It includes but is not limited to employees.

Data Controller

The organisation storing and controlling such information (i.e. the Charity) is referred to as the Data Controller.

Processing

Processing data involves any activity that involves the use of personal data. This includes but is not limited to: obtaining, recording or holding data or carrying out any operation or set of operations on that data such as organisation, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.

Automated Processing

Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

An example of automated processing includes profiling and automated decision making. Automatic decision making is when a decision is made which is based solely on automated processing (without human intervention) which produces legal effects or significantly affects an individual. Automated decision making is prohibited except in exceptional circumstances.

Data Protection Impact Assessment (DPIA)

DPIAs are a tool used to identify risks in data processing activities with a view to reducing them.

Data Breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Pseudonymised

The process by which personal data is processed in such a way that that it cannot be used to identify an individual without the use of additional data, which is kept separately and subject to technical and organisational measures to ensure that the personal data cannot be attributed to an identifiable individual.

When can Charity process personal data?

Data Protection Principles

The Charity is responsible for and adhere to the principles relating to the processing of personal data as set out in the UK GDPR. The principles the Charity must adhere to are set out below.

Principle 1: Personal data must be processed lawfully, fairly and in a transparent manner

The Charity only collect, process and share personal data fairly and lawfully and for specified purposes. The Charity must have a specified purpose for processing personal data and special category data as set out in the UK GDPR.

Before the processing starts for the first time we will review the purposes of the particular processing activity and select the most appropriate lawful basis for that processing. We will then regularly review those purposes whilst processing continues in order to satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose).

Personal Data

The Charity may only process a data subject's personal data if one of the following fair processing conditions are met: -

- The data subject has given their consent;
- The processing is necessary for the performance of a contract with the data subject or for taking steps at their request to enter into a contract;
- To protect the data subject's vital interests;
- To meet our legal compliance obligations (other than a contractual obligation);
- To perform a task in the public interest or in order to carry out official functions as authorised by law;
- For the purposes of the Charity's legitimate interests where authorised in accordance with data protection legislation. This is provided that it would not prejudice the rights and freedoms or legitimate interests of the data subject.

Special Category Data

The Charity may only process special category data if they are entitled to process personal data (using one of the fair processing conditions above) AND one of the following conditions are met:

- The data subject has given their explicit consent;

- The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed on the Charity in the field of employment law, social security law or social protection law. This may include, but is not limited to, dealing with sickness absence, dealing with disability and making adjustments for the same, arranging private health care insurance and providing contractual sick pay;
- To protect the data subject's vital interests;
- The processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
- Where the data has been made public by the data subject;
- To perform a task in the substantial public interest or in order to carry out official functions as authorised by law;
- Where it is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;
- Where it is necessary for reasons of public interest in the area of public health;
- The processing is necessary for archiving, statistical or research purposes.

The Charity identifies and documents the legal grounds being relied upon for each processing activity.

Criminal Record Data

Where criminal records data is processed, a lawful condition for processing that data is also identified and documented.

Consent

Where the Charity relies on consent as a fair condition for processing (as set out above), it will adhere to the requirements set out in the UK GDPR.

Consent must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they signify agreement to the processing of personal data relating to them. Explicit consent requires a very clear and specific statement to be relied upon (i.e. more than just mere action is required).

A data subject will have consented to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity will not amount to valid consent.

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured.

In cases of processing special category data and explicit consent, the Charity will normally seek another legal basis to process that data. However, if explicit consent is required, the data subject will be provided with full information in order to provide explicit consent.

The Charity will keep records of consents obtained in order to demonstrate compliance with consent requirements under the UK GDPR.

Principle 2: Personal data must be collected only for specified, explicit and legitimate purposes

Personal data will not be processed in any matter that is incompatible with the legitimate purposes specified.

The Charity will not use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the data subject of the new purpose (and they have consented where necessary).

Principle 3: Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed

The Charity will only process personal data when our obligations and duties require us to. We will not collect excessive data and ensure any personal data collected is adequate and relevant for the intended purposes.

When personal data is no longer needed for specified purposes, the Charity shall delete or anonymise the data. Please refer to the Charity's Data Retention Policy for further guidance.

Principle 4: Personal data must be accurate and, where necessary, kept up to date

The Charity will endeavour to correct or delete any inaccurate data being processed by checking the accuracy of the personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out of date personal data.

Data subjects also have an obligation to ensure that their data is accurate, complete, up to date and relevant. Data subjects have the right to request rectification to incomplete or inaccurate data held by the Charity.

Principle 5: Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed

Legitimate purposes for which the data is being processed may include satisfying legal, accounting or reporting requirements. The Charity will ensure that they adhere to legal timeframes for retaining data.

We will take reasonable steps to destroy or erase from our systems all personal data that we no longer require. We will also ensure that data subjects are informed of the period for which data is stored and how that period is determined in our privacy notices.

Please refer to the Charity's Retention Policy for further details about how the Charity retains and removes data.

Principle 6: Personal data must be processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage

In order to assure the protection of all data being processed, the Charity will develop, implement and maintain reasonable safeguard and security measures. This includes using measures such as: -

- Encryption;
- Pseudonymisation (this is where the Charity replaces information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure);
- Ensuring authorised access on both hard copy and electronic files (i.e. that only people who have a need to know the personal data are authorised to access it);
- Adhering to confidentiality principles;
- Ensuring personal data is accurate and suitable for the process for which it is processed.

The Charity follow procedures and technologies to ensure security and will regularly evaluate and test the effectiveness of those safeguards to ensure security in processing personal data.

The Charity will only transfer personal data to third party service providers who agree to comply with the required policies and procedures and agree to put adequate measures in place.

Sharing Personal Data

The Charity will generally not share personal data with third parties unless certain safeguards and contractual arrangements have been put in place. The following points will be considered:

- Whether the third party has a need to know the information for the purposes of providing the contracted services;

- Whether sharing the personal data complies with the privacy notice that has been provided to the data subject and, if required, the data subject's consent has been obtained;
- Whether the third party has agreed to comply with the required data security standards, policies and procedures and implemented adequate security measures;
- Whether the third party has agreed to comply with the required data security standards, policies and procedures and implemented adequate security measures;
- Whether the transfer complies with any applicable cross border transfer restrictions; and
- Whether a fully executed written contract that contains UK GDPR approved third party clauses has been obtained.

There may be circumstances where the Charity is required either by law or in the best interests of our pupils, parents or staff to pass information onto external authorities, for example, the Local Authority, Ofsted or the department of health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

The intention to share data relating to individuals to an organisation outside of the Charity shall be clearly defined within written notifications including details and the basis for sharing the data.

Transfer of Data Outside the European Economic Area (EEA)

The UK GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined.

The Charity will not transfer data to another country outside of the EEA without appropriate safeguards being in place and in compliance with the UK GDPR. All staff must comply with the Charity's guidelines on transferring data outside of the EEA. For the avoidance of doubt, a transfer of data to another country can occur when you transmit, send, view or access that data in that particular country.

Transfer of Data Outside the UK

The Charity may transfer personal information outside the UK and/or to international organisations on the basis that the country, territory or organisation is designated as having an adequate level of protection. Alternatively, the organisation receiving the information has provided adequate safeguards by way of binding corporate rules, Standard Contractual Clauses or compliance with an approved code of conduct.

Data Subject's Rights and Requests

Personal data must be made available to data subjects as set out within this policy and data subjects must be allowed to exercise certain rights in relation to their personal data.

The rights data subjects have in relation to how the Charity handle their personal data are set out below:

a) (Where consent is relied upon as a condition of processing) To withdraw consent to processing at any time;

b) Receive certain information about the Charity's processing activities;

c) Request access to their personal data that we hold (see "Subject Access Requests" at Appendix 1);

d) Prevent our use of their personal data for marketing purposes;

e) Ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;

f) Restrict processing in specific circumstances;

g) Challenge processing which has been justified on the basis of our legitimate interests or in the public interest;

h) Request a copy of an agreement under which personal data is transferred outside of the EEA;

i) Object to decisions based solely on automated processing;

j) Prevent processing that is likely to cause damage or distress to the data subject or anyone else;

k) Be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;

l) Make a complaint to the supervisory authority; which is the Information Commissioner in England and Wales https://ico.org.uk/global/contact-us/; and

m) In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

If any request is made to exercise the rights above, it is a requirement for the relevant staff member within the Charity to verify the identity of the individual making the request.

Direct Marketing

The Charity is subject to certain rules and privacy laws when marketing. For example, a data subject's prior consent will be required for electronic direct marketing (for example, by email, text or automated calls).

The Charity will explicitly offer individuals the opportunity to object to direct marketing and will do so in an intelligible format which is clear for the individual to understand. The Charity will promptly respond to any individual objection to direct marketing.

Employee Obligations

Employees may have access to the personal data of other members of staff, suppliers, service users, parents or students of the Charity in the course of their employment or engagement. If so, the Charity expects those employees to help meet the Charity's data protection obligations to those individuals. Specifically, you must: -

- Only access the personal data that you have authority to access, and only for authorised purposes;
- Only allow others to access personal data if they have appropriate authorisation;
- Keep personal data secure (for example, by complying with rules on access to Charity's premises, computer access, password protection and secure file storage and destruction. Please refer to the ICT Acceptable Use Policy for further details about our security processes;
- Not remove personal data or devices containing personal data from the Charity's premises unless appropriate security measures are in place (such as pseudonymisation, encryption, password protection) to secure the information;
- Not store personal information on local drives.

Accountability

The Charity will ensure compliance with data protection principles by implementing appropriate technical and organisational measures. We are responsible for and demonstrate accountability with the UK GDPR principles.

The Charity have taken the following steps to ensure and document UK GDPR compliance:-

Data Protection Officer (DPO)
Please find below details of the Charity s Data Protection Officer: -
Data Protection Officer: Judicium Consulting Limited
Address: 5th Floor, 98 Theobalds Road, London, WC1X 8WB
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Telephone: 0345 548 7000 option 1 then option 1 again

The DPO is responsible for overseeing this Data Protection Policy and developing data-related policies and guidelines.

Please contact the DPO with any questions about the operation of this Data Protection Policy or the UK GDPR or if you have any concerns that this policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances: -

(a) If you are unsure of the lawful basis being relied on by the Charity to process personal data;

(b) If you need to rely on consent as a fair reason for processing (please see below the section on consent for further detail);

(c) If you need to draft privacy notices or fair processing notices;

(d) If you are unsure about the retention periods for the personal data being processed

(e) If you are unsure about what security measures need to be put in place to protect personal data;

(f) If there has been a personal data breach

(g) If you are unsure on what basis to transfer personal data outside the EEA;

(h) If you need any assistance dealing with any rights invoked by a data subject;

(i) Whenever you are engaging in a significant new (or a change in) processing activity which is likely to require a data protection impact assessment or if you plan to use personal data for purposes other than what it was collected for;

(j) If you plan to undertake any activities involving automated processing or automated decision making;

(k) If you need help complying with applicable law when carrying out direct marketing activities;

(l) If you need help with any contracts or other areas in relation to sharing personal data with third parties.

Personal Data Breaches

The UK GDPR requires the Charity to notify any applicable personal data breach to the Information Commissioner's Office (ICO).

We have put in place procedures to deal with any suspected personal data breach and will notify data subjects or any applicable regulator where we are legally required to do so. Please refer to our Data Breach policy.

If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the person designated as the key point of contact for personal data breaches in your area or your DPO.

Transparency and Privacy Notices

The Charity will provide detailed, specific information to data subjects. This information will be provided through the Charity's privacy notices which are concise, transparent, intelligible, easily accessible and in clear and plain language so that a data subject can easily understand them. The Charity's privacy notices are tailored to suit the data subject and set out information about how the Charity use their data.

Whenever we collect personal data directly from data subjects, including for human resources or employment purposes, we will provide the data subject with all the information required by the UK GDPR. This includes the identity of the Data Protection Officer, the Charity's contact details, how and why we will use, process, disclose, protect and retain personal data. This information will be provided within our privacy notices.

When personal data is collected indirectly (for example, from a third party or a publicly available source), where appropriate, we will provide the data subject with the above information as soon as possible after receiving the data. The Charity will also confirm whether that third party has collected and processed data in accordance with the UK GDPR.

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as "children" under the UK GDPR.

Privacy by Design

The Charity adopt a privacy by design approach to data protection to ensure that we adhere to data compliance and to implement technical and organisational measures in an effective manner.

Privacy by design is an approach that promotes privacy and data protection compliance from the start. To help us achieve this, the Charity takes into account the nature and purposes of the processing, any cost of implementation and any risks to rights and freedoms of data subjects when implementing data processes.

Data Protection Impact Assessments (DPIAs)

In order to achieve a privacy by design approach, the Charity conduct DPIAs for any new high risk technologies or programmes being used by the Charity which could affect the processing of personal data. The Charity carries out DPIAs when required by the UK GDPR in the following circumstances: -

- For the use of new technologies (programs, systems or processes) or changing technologies;
- For the use of automated processing;
- For large scale processing of special category data; and
- For large scale, systematic monitoring of a publicly accessible area (through the use of CCTV).

Our DPIAs contain: -

- A description of the processing, its purposes and any legitimate interests used;
- Details of what types of data are shared;
- Steps taken by the third party and the Charity in order to protect data;
- An assessment of the necessity and proportionality of the processing in relation to its purpose;
- An assessment of the risk to individuals; and
- The risk mitigation measures in place and demonstration of compliance.

Record Keeping

The Charity are required to keep full and accurate records of our data processing activities. These records include: -

- The name and contact details of the Charity;
- The name and contact details of the Data Protection Officer;
- Descriptions of the types of personal data used;
- Description of the data subjects;
- Details of the Charity's processing activities and purposes;
- Details of any third party recipients of the personal data;
- Where personal data is stored;
- Retention periods; and
- Security measures in place.

Training

The Charity will ensure all relevant personnel have undergone adequate training to enable them to comply with data privacy laws. The Charity will carry out adequate training with all staff annually

Audit

The Charity, through its Data Protection Officer, regularly test our data systems and processes in order to assess compliance. These are done through data audits which take place regularly in order to review use of personal data.

Underpinning Policies & Procedures

More information can be found in:

- the ICT Acceptable Use Policy
- Bring Your Own Device Policy
- Remote Access Policy
- Data Breach Policy
- Back Up and Restore Policy
- Employee Code of Conduct
- Business Continuity Plan
- Staff Privacy Notice
- Student Privacy Notice
- Service User Privacy Notices
- Visitor Privacy Notice
- Website Visitor Privacy Notice

We will monitor the effectiveness of this and all of our policies and procedures and conduct a full review and update as appropriate.

Our monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to the Charity.

National Data Opt-out

From March 2022, all regulated social care providers in England will need to comply with the national data opt-out. Under the national data opt-out everyone who uses publicly-funded health and/or care services can stop health and care organisations from sharing their "confidential patient information" with other organisations if it is not about managing or delivering their own care. For example, if this information is used for research or planning purposes.

The Charity does not share confidential patient/service user information outside of the managing or delivering their own care, therefore is out of scope of the National Data Opt-out requirement. This will be reviewed annually and adapted when required.

Appendix 1 – Subject Access Requests

Under Data Protection Law, Data Subjects have a general right to find out whether the Charity hold or process personal data about them, to access that data, and to be given supplementary information. This is known as the right of access, or the right to make a data subject access request (SAR). The purpose of the right is to enable the individual to be aware of, and verify, the lawfulness of the processing of personal data that the Charity is undertaking. It is designed to assist individuals in understanding how and why we are using their data and to check that we are doing so lawfully. The main provisions are to be found in Articles 12 and 15 of the UK GDPR and Section 45 of the Data Protection Act 2018.

This appendix provides guidance for staff members on how data subject access requests should be handled, and for all individuals on how to make a SAR.

Failure to comply with the right of access under UK GDPR puts both staff and the Charity at potentially significant risk, and so the Charity takes compliance with this policy very seriously.

A Data Subject has the right to be informed by the Charity of the following: -

(a) Confirmation that their data is being processed;

(b) Access to their personal data;

(c) A description of the information that is being processed;

(d) The purpose for which the information is being processed;

(e) The recipients/class of recipients to whom that information is or may be disclosed;

(f) Details of the Charity's sources of information obtained;

(g) In relation to any Personal Data processed for the purposes of evaluating matters in relation to the Data Subject that has constituted or is likely to constitute the sole basis for any decision significantly affecting him or her, to be informed of the logic of the Data Controller's decision making. Such data may include, but is not limited to, performance at work, creditworthiness, reliability and conduct; and

(h) Other supplementary information.

Dealing with a SAR is time critical and must be prioritised. Other than in exceptional cases, we will have only one month in which to respond to a SAR and even if an extension of the time limit is permitted, the individual must still be informed within that month of the fact that the request will take longer to process and the reasons for the delay. Failure to deal with a SAR within that period could leave us open to the possibility of being fined by the ICO.

All staff must be aware of the potential for receiving a SAR and the importance of dealing with such as request as a matter of urgency.

Anyone within the Charity may receive a SAR. It does not need to be made to a nominated person or even to a person responsible for dealing with either the data subject or information of that type. It will be equally as valid if sent to anyone within the Charity.

If you receive a SAR, please contact Head of MIS, or if not available, your Data Protection Link . A request for information does not need to mention that it is a SAR provided that it is clear that it is an individual asking for their own personal data. There is no specified wording and it does not have to be on an official form. A SAR does not need to be in writing and can be made verbally, by post, by email or even using social media where relevant.

How to recognise a subject access request

A data subject access request is a request from an individual (or from someone acting with the authority of an individual, e.g. a solicitor or a parent making a request in relation to information relating to their child):

- for confirmation as to whether the Charity process personal data about them and, if so
- for access to that personal data
- and/or certain other supplementary information

A valid SAR can be both in writing (by letter, email, WhatsApp text) or verbally (e.g. during a telephone conversation). The request may refer to the UK GDPR and/or to 'data protection' and/or to 'personal data' but does not need to do so in order to be a valid request. For example, a letter which states 'please provide me with a copy of information that the Charity hold about me' will be a data subject access request and should be treated as such.

A data subject is generally only entitled to access their own personal data, and not information relating to other people.

How to make a data subject access request

Whilst there is no requirement to do so, we encourage any individuals who wish to make such a request to make the request in writing, detailing exactly the personal data being requested. This allows the Charity to easily recognise that you wish to make a data subject access request and the nature of your request. If the request is unclear/ vague we may be required to clarify the scope of the request which may in turn delay the start of the time period for dealing with the request.

If a request is made verbally, we will ensure we follow this up with something in writing to confirm what has been requested and outline the timeframe for dealing with the request.

What to do when you receive a data subject access request

All data subject access requests should be immediately directed to Head of MIS, or if not available, your Data Protection Link who should contact Judicium as DPO in order to assist with the request and what is required. There are limited timescales within which the Charity must respond to a request and any delay could result in failing to meet those timescales, which could lead to enforcement action by the Information Commissioner's Office (ICO) and/or legal action by the affected individual without delay. If ever in doubt, please refer the request to Head of MIS.

Acknowledging the request

When receiving a SAR the Charity shall acknowledge the request as soon as possible and inform the requester about the statutory deadline (of one calendar month) to respond to the request.

In addition to acknowledging the request, the Charity may ask for:

- proof of ID (if needed);
- further clarification about the requested information if it is not clear what information is required;
- if it is not clear where the information shall be sent, the Charity must clarify what address/email address to use when sending the requested information; and/or
- consent (if requesting third party data).

The Charity should work with their DPO in order to create the acknowledgment.

Verifying the identity of a requester or requesting clarification of the request

Before responding to a SAR, the Charity will take reasonable steps to verify the identity of the person making the request. In the case of current employees, this will usually be straightforward. The Charity is entitled to request additional information from a requester in

order to verify whether the requester is in fact who they say they are. Where the Charity has reasonable doubts as to the identity of the individual making the request, evidence of identity may be established by production of a passport, driving license, a recent utility bill with current address, birth/marriage certificate, credit card or a mortgage statement.

If an individual is requesting a large amount of data the Charity may ask the requester for more information for the purpose of clarifying the request, but the requester shall never be asked why the request has been made. The Charity shall let the requestor know as soon as possible where more information is needed before responding to the request.

When it is necessary to verify the identity of the person making the request, the one calendar month period for responding begins when sufficient confirmation of identity is provided.

When it is necessary to request more information for the purpose of clarifying the request, the one calendar month period for responding pauses when further information is requested and does not restart until sufficient clarification is provided.

In both cases, the period of responding begins when the additional information has been received. If the Charity do not receive this information, they will be unable to comply with the request.

Requests made by third parties or on behalf of children

The Charity need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney. The Charity may also require proof of identity in certain circumstances.

If the Charity is in any doubt or has any concerns as to providing the personal data of the data subject to the third party, then it should provide the information requested directly to the data subject. It is then a matter for the data subject to decide whether to share this information with any third party.

When requests are made on behalf of children, it is important to note that even if a 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 have access to the child's personal data. Before responding to a SAR for information held about a child, the Charity should consider whether the child is mature enough to understand their rights. If the Charity is confident that the child can understand their rights, then the Charity should usually respond directly to the child or seek their consent before releasing their information.

It shall be assessed if the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, it should be taken into account, among other things:

- 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.

Generally, a person aged 12 years or over is presumed to be of sufficient age and maturity to be able to exercise their right of access, unless the contrary is shown. In relation to a child 12 years of age or older, then provided that the Charity is confident that they understand their rights, and there is no reason to believe that the child does not have the capacity to make a request on their own behalf, the Charity will require the written authorisation of the child before responding to the requester, or provide the personal data directly to the child.

The Charity may also refuse to provide information to parents if there are consequences of allowing access to the child's information – for example if it is likely to cause detriment to the child.

Fee for responding to a SAR

The Charity will usually deal with a SAR free of charge. Where a request is considered to be manifestly unfounded or excessive a fee to cover administrative costs may be requested. If a request is considered to be manifestly unfounded or unreasonable the Charity will inform the requester why this is considered to be the case and that the Charity will charge a fee for complying with the request.

A fee may also be requested in relation to repeat requests for copies of the same information. In these circumstances a reasonable fee will be charged taking into account the administrative costs of providing the information. If a fee is requested, the period of responding begins when the fee has been received.

Time Period for Responding to a SAR

The Charity has one calendar month to respond to a SAR. This will run from the day that the request was received or from the day when any additional identification or other information requested is received, or payment of any required fee has been received.

The circumstances where the Charity is in any reasonable doubt as to the identity of the requester, this period will not commence unless and until sufficient information has been provided by the requester as to their identity, and in the case of a third party requester, the written authorisation of the data subject has been received.

The period for response may be extended by a further two calendar months in relation to complex requests. What constitutes a complex request will depend on the particular nature of the request. The DPO must always be consulted in determining whether a request is sufficiently complex as to extend the response period.

Where a request is considered to be sufficiently complex as to require an extension of the period for response, the Charity will need to notify the requester within one calendar month of receiving the request, together with reasons as to why this extension is considered necessary.

Information to be provided in response to a request

The individual is entitled to receive access to the personal data we process about him or her and the following information:

- the purpose for which we process the data;
- the recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular where those recipients are in third countries or international organisations;
- where possible, the period for which it is envisaged the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the fact that the individual has the right:
    - to request that the Company rectifies, erases or restricts the processing of his personal data; or
    - to object to its processing;
    - to lodge a complaint with the ICO;
    - where the personal data has not been collected from the individual, any information available regarding the source of the data;
    - any automated decision we have taken about him or her together with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for him or her.

The information should be provided in a way that is concise, transparent, easy to understand and easy to access using clear and plain language, with any technical terms, abbreviations or codes explained. The response shall be given in writing if the SAR was made in writing in a commonly-used electronic format.

The information that the Charity is required to supply in response to a SAR must be supplied by reference to the data in question at the time the request was received. However, as the Charity have one month in which to respond the Charity is allowed to take into account any amendment or deletion made to the personal data between the time the request is received and the time the personal data is supplied if such amendment or deletion would have been made regardless of the receipt of the SAR.

The Charity is therefore, allowed to carry out regular housekeeping activities even if this means deleting or amending personal data after the receipt of a SAR. The Charity is not allowed to amend or delete data to avoid supplying the data.

How to locate information

The personal data the Charity need to provide in response to a data subject access request may be located in several of the electronic and manual filing systems. This is why it is important to identify at the outset the type of information requested so that the search can be focused.

Depending on the type of information requested, the Charity may need to search all or some of the following:

- electronic systems, e.g. databases, networked and non-networked computers, servers, customer records, human resources system, email data, back up data, CCTV;
- manual filing systems in which personal data is accessible according to specific criteria, e.g. chronologically ordered sets of manual records containing personal data;
- data systems held externally by our data processors;
- safeguarding systems (such as CPOMS);
- MIS system (such as Databridge);
- occupational health records;
- pensions data;
- share scheme information;
- insurance benefit information.

The Charity should search these systems using the individual's name, employee number or other personal identifier as a search determinant.

Protection of third parties -exemptions to the right of subject access

There are circumstances where information can be withheld pursuant to a SAR. These specific exemptions and requests should be considered on a case by case basis.

The Charity will consider whether it is possible to redact information so that this does not identify those third parties. If their data cannot be redacted (for example, after redaction it is still obvious who the data relates to) then the Charity do not have to disclose personal data to the extent that doing so would involve disclosing information relating to another individual (including information identifying the other individual as the source of information) who can be identified from the information unless:

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

In determining whether it is reasonable to disclose the information without the individuals consent, all of the relevant circumstances will be taken into account, including:

- the type of information that they would disclose;
- any duty of confidentiality they owe to the other individual;
- any steps taken to seek consent from the other individual;
- whether the other individual is capable of giving consent; and
- any express refusal of consent by the other individual.

It needs to be decided whether it is appropriate to disclose the information in each case. This decision will involve balancing the data subject's right of access against the other individual's rights. If the other person consents to the Charity disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, the Charity must decide whether to disclose the information anyway. If there are any concerns in this regard then the DPO should be consulted.

Other exemptions to the right of subject access

In certain circumstances the Charity may be exempt from providing some or all of the personal data requested. These exemptions are described below and should only be applied on a case-by-case basis after a careful consideration of all the facts.

Crime detection and prevention: The Charity do not have to disclose any personal data being processed for the purposes of preventing or detecting crime; apprehending or prosecuting offenders; or assessing or collecting any tax or duty.

Confidential references: The Charity do not have to disclose any confidential references given to third parties for the purpose of actual or prospective:

- education, training or employment of the individual;
- appointment of the individual to any office; or
- provision by the individual of any service

This exemption does not apply to confidential references that the Charity receive from third parties. However, in this situation, granting access to the reference may disclose the personal data of another individual (i.e. the person giving the reference), which means that the Charity must consider the rules regarding disclosure of third-party data set out above before disclosing the reference.

Legal professional privilege: The Charity do not have to disclose any personal data which are subject to legal professional privilege.

Management forecasting: The Charity do not have to disclose any personal data processed for the purposes of management forecasting or management planning to assist us in the conduct of any business or any other activity.

Negotiations: The Charity do not have to disclose any personal data consisting of records of intentions in relation to any negotiations with the individual where doing so would be likely to prejudice those negotiations.

Refusing to respond to a request

The Charity can refuse to comply with a request if the request in certain circumstances. These include:

Where the SAR is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature;

To avoid obstructing an official or legal inquiry, investigation or procedure;

To avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

To protect public security;

To protect national security;

To protect the rights and freedoms of others.

In the event that you have concerns about supplying the information, you must always refer the matter to Head of MIS who will make the decision on our behalf.

In the event that we decide not to comply with the SAR, then the data subject must be informed, without undue delay (and in all cases within one month of receipt of the request), of:

The reasons we are not taking action;

That they have a right to make a complaint to the ICO or another supervisory authority; and

That they are entitled to seek to enforce their right through a judicial remedy.

If a request is found to be manifestly unfounded or excessive the Charity can:

request a "reasonable fee" to deal with the request; or

refuse to deal with the request.

In either case the Charity need to justify the decision and inform the requestor about the decision.

The reasonable fee should be based on the administrative costs of complying with the request. If deciding to charge a fee the Charity should contact the individual promptly and inform them. The Charity do not need to comply with the request until the fee has been received.

Record keeping

A record of all subject access requests shall be kept by the Head of MIS. The record shall include the date the SAR was received, the name of the requester, what data the Charity sent to the requester and the date of the response.

Appendix 2 – Subject Access Request Form

The Data Protection Act 2018 provides you, the data subject, with a right to receive a copy of the data/information we hold about you or to authorise someone to act on your behalf. Please complete this form if you wish to make a request for your data. Your request will normally be processed within one calendar month upon receipt of a fully completed form and proof of identity.

Proof of Identity

We require proof of your identity before we can disclose personal data. Proof of your identity should include a copy of a document such as your birth certificate, passport, driving licence, official letter addressed to you at your address e.g., bank statement, recent utilities bill or council tax bill. The document should include your name, date of birth and current address. If you have changed your name, please supply relevant documents evidencing the change.

Section 1

Please fill in the details of the data subject (i.e., the person whose data you are requesting). If you are not the data subject and you are applying on behalf of someone else, please fill in the details of the data subject below and not your own.

Title	
Surname/Family Name	
First Name(s)/ Forename	
Date of Birth	
Address	
Post Code	
Phone Number	
Email address	

I am enclosing the following copies as proof of identity (please tick the relevant box):

- ☐ Birth certificate
- ☐ Driving licence
- ☐ Passport
- ☐ An official letter to my address

Personal Information

If you only want to know what information is held in specific records, please indicate in the box below. Please tell us if you know in which capacity the information is being held, together with any names or dates you may have. If you do not know exact dates, please give the year(s) that you think may be relevant.

Details:

Employment records:

If you are, or have been employed by the Charity and are seeking personal information in relation to your employment please provide details of your staff number, unit, team, dates of employment etc.

Details:

Section 2

Please complete this section of the form with your details if you are acting on behalf of someone else (i.e., the data subject).

If you are **NOT** the data subject, but an agent appointed on their behalf, you will need to provide evidence of your identity as well as that of the data subject and proof of your right to act on their behalf.

Title	
Surname/ Family Name	
First Name(s)/Forenames	
Date of Birth	
Address	
Post Code	
Phone Number	

I am enclosing the following copies as proof of identity (please tick the relevant box):

- ☐ Birth certificate
- ☐ Driving licence
- ☐ Passport
- ☐ An official letter to my address

What is your relationship to the data subject? (e.g., parent, carer, legal representative)

I am enclosing the following copy as proof of legal authorisation to act on behalf of the data subject:

- ☐ Letter of authority
- ☐ Lasting or Enduring Power of Attorney
- ☐ Evidence of parental responsibility
- ☐ Other (give details):

Section 3

Please describe as detailed as possible what data you request access to (e.g., time period, categories of data, information relating to a specific case, paper records, electronic records).

I wish to:

- ☐ Receive the information by post*
- ☐ Receive the information by email
- ☐ Collect the information in person
- ☐ View a copy of the information only
- ☐ Go through the information with a member of staff

*Please be aware that if you wish us to post the information to you, we will take every care to ensure that it is addressed correctly. However, we cannot be held liable if the information is lost in the post or incorrectly delivered or opened by someone else in your household. Loss or incorrect delivery may cause you embarrassment or harm if the information is 'sensitive'.

Please send your completed form and proof of identity by email to: dataprotection@hensahws.org.uk

Appendix 3

EIA Form

Question	Response
Name of policy	Data Protection Policy
Summary of aims and objectives of the policy	See *Aim and scope of policy* section on Page 1 of the policy
What involvement and consultation has been done in relation to this policy? *(e.g. with relevant groups and stakeholders)*	Policy is based on a template provided by Judicium Education, Henshaws' Data Protection Officer. Charity's Data Protection Working Group reviewed and adjusted the policy to meet needs of the organisation Judicium Education reviewed and approved the adjusted policy
Who is affected by the policy	All staff and people supported by Henshaws, volunteers, agency, everyone sharing personal information with Henshaws
What are the arrangements for monitoring and reviewing the actual impact of the policy	Annual review by HSMT, Charity's Data Protection Working Group and Judicium Education during annual audit

Protected Characteristic Group	Is there a potential for positive or negative impact?	Please explain and give examples of any evidence/data used	Action to address negative impact (e.g. adjustment to the policy)/Lead/Timescale
Disability	Neutral	Applies to all staff with no advantage/disadvantage specific groups	
Gender reassignment	Neutral	Applies to all staff with no advantage/disadvantage specific groups	
Marriage or civil partnership	Neutral	Applies to all staff with no advantage/disadvantage specific groups	
Pregnancy & Maternity	Neutral	Applies to all staff with no advantage/disadvantage specific groups	
Race	Neutral	Applies to all staff with no advantage/disadvantage specific groups	
Religion or belief	Neutral	Applies to all staff with no advantage/disadvantage specific groups	
Sexual orientation	Neutral	Applies to all staff with no advantage/disadvantage specific groups	
Sex (gender)	Neutral	Applies to all staff with no advantage/disadvantage specific groups	

Age	Neutral	Applies to all staff with no advantage/disadvantage specific groups	

Question	Explanation/Justification	
Is it possible the proposed policy or activity or change in policy or activity could discriminate or unfairly disadvantage people?	No disadvantage/advantage apparent.	
Final Decision:	**Tick the relevant box**	**Include any explanation / justification required**
1. No barriers identified, therefore activity will **proceed.**	X	
2. **Stop** the policy or practice at some point because the data shows bias towards one or more groups		
3. **Adapt or change** the policy in a way which you think will eliminate the bias		
4. Barriers and impact identified, however having considered all available options carefully, there appear to be no other proportionate ways to achieve the aim of the policy or practice (e.g. in extreme cases or where positive action is taken). Therefore you are going to **proceed with caution** with this policy or practice knowing that it may favour some people less than others, providing justification for this decision.		