.henshaws
beyond expectations

DP001 DATA BREACH POLICY

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

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

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

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	Change of roles, updated template from Judicium expanding number of sections with more detail.
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 Protection 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 one
Suggested Action	Disseminate to all staff, publish on the website

.henshaws
beyond expectations

Data Breach Policy

The UK General Data Protection Regulation (UK GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The UK GDPR places obligations on staff to report actual or suspected data breaches and our procedure for dealing with breaches is set out below. All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Training will be provided to all staff to enable them to carry out their obligations within this policy.

Data Processors will be provided with a copy of this policy and will be required to notify the Charity of any data breach without undue delay after becoming aware of the data breach. Failure to do so may result in a breach to the terms of the processing agreement.

Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the Charity's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

This policy does not form part of any individual's terms and conditions of employment with the Charity and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

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

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data or special category data transmitted, stored or otherwise processed.

Data Subject
Person to whom the personal data relates.

ICO
The ICO is the Information Commissioner's Office, the UK's independent regulator for data protection and information.

Responsibility
Head of MIS has overall responsibility for breach notification within the Charity. They are responsible for ensuring breach notification processes are adhered to by all staff and are the designated point of contact for personal data breaches.

In the absence of Head of MIS, please contact your Data Protection
Link or dataprotection@henshaws.org.uk.

The Data Protection Officer (DPO) is responsible for overseeing this policy and developing data-related policies and guidelines.

Please contact the DPO with any questions about the operation of this policy or the UK GDPR or if you have any concerns that this policy is not being or has not been followed.

The DPO's contact details are set out below: -

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 opt 1, then opt 1

Security and Data Related Policies

We must keep personal data secure against loss or misuse. All staff are required to comply with our information security guidelines and policies. Staff should refer to the following policies that are related to this Data Breach Policy: -

- Bring Your Own Device Policy
- ICT Acceptable Use Policy
- Remote Access Policy
- Data Protection Policy which sets out the Charity's obligations under UK GDPR about how they process personal data.

These policies are also designed to protect personal data and can be found at [N:\SOCIETY\POLICIES & PROCEDURES\Data Protection and N:\Society\POLICIES & PROCEDURES\IT].

Data Breach Procedure

What is a personal data breach?

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.

Examples of a data breach could include the following (but are not exhaustive): -

- Loss or theft of data or equipment on which data is stored for example, loss of a laptop or a paper file (this includes accidental loss);
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Human error (for example, sending an email or SMS to the wrong recipient);
- Unforeseen circumstances such as a fire or flood;
- Hacking, phishing and other "blagging" attacks where information is obtained by deceiving whoever holds it.
- Alteration of personal data without permission;
- Loss of availability of personal data.

When does it need to be reported?

The Charity must notify the ICO of a data breach where it is likely to result in a risk to the rights and freedoms of individuals. This means that the breach needs to be more than just losing personal data and if unaddressed, the breach is likely to have a significant detrimental effect on individuals.

Examples of where the breach may have a significant effect includes: -

- Potential or actual discrimination;
- Potential or actual financial loss;
- Potential or actual loss of confidentiality;
- Risk to physical safety or reputation;
- Exposure to identity theft (for example, through the release of non-public identifiers such as passport details); and
- The exposure of the private aspect of a person's life becoming known by others.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, then the individuals must also be notified directly.

Reporting a Data Breach

If you know or suspect a personal data breach has occurred or may occur which meets the criteria above, you should: -

- In first instance contact Head of MIS, or if not available, your Data Protection Link, who will gather information from you and contact Charity's DPO, Judicium Consulting Limited, for advice and guidance

Breach reporting is encouraged throughout the Charity and staff are expected to seek advice if they are unsure as to whether the breach should be reported and/or could result in a risk to the rights and freedom of individuals. They can seek advice from their line manager, Head of MIS, Data Protection Link or the DPO.

Once reported, you should not take any further action in relation to the breach. In particular you must not notify any affected individuals or regulators or investigate further. Head of MIS will acknowledge receipt of the data breach information and take appropriate steps to deal with the report in collaboration with the DPO.

Managing and Recording the Breach

On being notified of a suspected personal data breach, Head of MIS, or in their absence Data Protection Link, will notify the DPO. Collectively they will take immediate steps to establish whether a personal data breach has in fact occurred. If so, they will take steps to:-

- Where possible, contain the data breach;
- As far as possible, recover, rectify or delete the data that has been lost, damaged or disclosed;
- Assess and record the breach in the Charity's data breach register;
- Notify the ICO where required;
- Notify data subjects affected by the breach if required;
- Notify other appropriate parties to the breach; and
- Take steps to prevent future breaches.

Containment and Recovery

Head of MIS with the support of our DPO will identify how the breach occurred and take immediate steps to stop of minimise further loss, destruction or unauthorised disclosure of personal data.

Chief Operating Officer with the support of our DPO will identify ways to recover, correct or delete data. This may include contacting the police, e.g., where the breach involves stolen hardware or data.

Depending on the nature of the breach, Chief Operating Officer with the support of our DPO, will notify the insurer, as the insurer can provide access to data breach management experts.

Notifying the ICO

Head of MIS with the support of our DPO will notify the ICO when a personal data breach has occurred which is likely to result in a risk to the rights and freedoms of individuals.

This will be done without undue delay and where possible, within 72 hours of becoming aware of the breach. The 72 hours deadline is applicable regardless of weekends and holidays (i.e., it is not 72 working hours). If the Charity are unsure of whether to report a breach, the assumption will be to report it.

Where the notification is not made within 72 hours of becoming aware of the breach, written reasons will be recorded as to why there was a delay in referring the matter to the ICO.

If the Charity are unsure whether to report, the presumption should be to report. The Charity will take into account of the factors set out below:

The potential harm to the rights and freedoms of data subjects

This is the overriding consideration in deciding whether a breach of data security should be reported to the ICO. Detriments include emotional distress as well as both physical and financial damage. It can include:

- Exposure to identify theft through the release of non-public identifiers, e.g. passport number;
- Information about the private aspects of a persons life becoming known to others, e.g. financial circumstances;

The personal data breach must be reported unless it is unlikely to result in a risk to data subjects' rights and freedoms.

The volume of personal data

There should be a presumption to report to the ICO where:

- A large volume of personal data is concerned; and
- There is a real risk to individuals suffering some harm.

It will, however, be appropriate to report much lower volumes in some circumstances where the risk is particularly high, e.g. because of the circumstances if the loss or the extent of information about each individual.

The sensitivity of data

There should be a presumption to report to the ICO where smaller amounts of personal data are involved, the release of which could cause a significant risk of individuals suffering substantial detriment, including substantial distress.

This is most likely to be the case where the breach involves special category personal data. If the information is particularly sensitive, even a single record could trigger a report. The ICO provides two examples:

- theft of a manual paper-based filing system (or unencrypted digital media) holding the personal data and financial records of 50 named individuals would be reportable;
- breach of a similar system holding the trade union subscription records of the same number of individuals (where there are no special circumstances surrounding the loss) would not be reportable.

Notifying Data Subjects

Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, Head of MIS will notify the affected individuals without undue delay including the name and contact details of the DPO and the ICO, the likely consequences of the data breach and the measures the Charity have (or intended) to take to address the breach, including where appropriate, recommendations for mitigating potential adverse effects.

When determining whether it is necessary to notify individuals directly of the breach, Head of MIS will co-operate with and seek guidance from the DPO, the ICO and any other relevant authorities (such as the police).

If it would involve disproportionate effort to notify the data subjects directly (for example, by not having contact details of the affected individual) then the Charity will consider alternative means to make those affected aware (for example, by making a statement on the Charity website).

Notifying the Police

Charity will already have considered whether to contact the police for the purpose of containment and recovery. Regardless of this, if it subsequently transpires that the breach arose from a criminal act, the Charity will notify the police and/or relevant law enforcement authorities.

Notifying Other Authorities

The Charity will need to consider whether other parties need to be notified of the breach. For example:

- The Information Commissioners Office (ICO);
- Affected data subjects;
- Insurers;
- Parents of college students;
- Third parties (for example, when they are also affected by the breach);
- Local authorities;
- The police (for example, if the breach involved theft of equipment or data).

This list is non-exhaustive.

Assessing the Breach

Once initial reporting procedures have been carried out, the Charity will carry out all necessary investigations into the breach.

The Charity will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal data. We will identify ways to recover, correct or delete data (for example, notifying our insurers or the police if the breach involves stolen hardware or data).

Having dealt with containing the breach, the Charity will consider the risks associated with the breach. These factors will help determine whether further steps need to be taken (for example notifying the ICO and/or data subjects as set out above). These factors include:

- What type of data is involved and how sensitive it is;
- The volume of data affected;
- Who is affected by the breach (i.e., the categories and number of people involved);
- The likely consequences of the breach on affected data subjects following containment and whether further issues are likely to materialise;
- Are there any protections in place to secure the data (for example, encryption, password protection, pseudonymisation, two factor authentication);
- What has happened to the data, e.g., if data has been stolen, could it be used for harmful purposes;
- What could the data tell a third party about the data subject;
- What are the likely consequences of the personal data breach on the Charity; and
- Any other wider consequences which may be applicable.

Preventing Future Breaches

Once the data breach has been dealt with, the Charity will consider its security processes with the aim of preventing further breaches. In order to do this, we will:

- Establish what security measures were in place when the breach occurred;
- Assess whether technical or organisational measures can be implemented to prevent the breach happening again;
- Consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice;
- Consider whether it is necessary to conduct a privacy or data protection impact assessment;
- Consider whether further audits or data protection steps need to be taken;
- To update the data breach register;
- To debrief governors/management following the investigation.

Reporting Data Protection Concerns

Prevention is always better than dealing with data protection as an after-thought. Data security concerns may arise at any time and we would encourage you to report any concerns (even if they do not meet the criteria of a data breach) that you may have to Chief Operating Officer, Head of

Mis, Data Protection Link or the DPO. This can help capture risks as they emerge, protect the Charity from data breaches and keep our processes up to date and effective.

Staff Awareness and Training

Key to the success of our systems is staff awareness and understanding. We provide regular training to staff:

- At induction;
- Annual refresher training;
- When significant new threats are identified; and
- In the event of an incident affecting our Charity.

Charity will ensure that staff are trained and aware on the need to report data breaches to ensure that they know to detect a data breach and the procedures of reporting them. This policy will be shared with staff.

Monitoring

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.

Appendix 1

EIA Form

Question	Response
Name of policy	Data Breach Policy
Summary of aims and objectives of the policy	See *Data Breach 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.		