



Data Protection

CHARITY POLICY & PROCEDURE

Document Revised:	April 2025
Ratified by Trustees:	April 2025
Next Review Date:	August 2026

Content

Aims

1. Legislation & Guidance
2. Data Definitions
3. The Data Controller
4. Roles and Responsibilities
5. Data Protection Principles
6. Personal Data Protection Principles
7. Individuals Other Rights and Subject Access Requests
8. Parental Requests to see Educational Records
9. Photographs and Videos
10. Artificial Intelligence (AI)
11. Data Security and Storage of Records
12. Data Retention and Disposal of Records
13. Personal Data Breaches
14. Training
15. Review

Appendix 1 – Personal Data Breach Procedure

Data Protection Policy

Aims

This **Data Protection Policy** is in place to ensure all employees, Trustees and Governors are aware of their responsibilities and outlines how the Charity complies with the following core data protection principles. It aims to set out how Talbot House Children's Charity ("The Charity") handles the personal data of our existing and former employees, agency staff, trustees and governors pupils, parents / carers, and other individual / third parties, including job applicants, visitors and contractors, all are referred to in this policy as relevant individuals.

This policy applies to the processing of personal data including manual (paper) and electronic (digital) records kept by the Charity in connection with its human resources function, as described below. It also covers the Charity's response to any data breach and other rights under the General Data Protection Regulation and current Data Protection Act.

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 GDPR 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, 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 current data protection legislation, the Charity understands that it will be accountable for the processing, management and regulation, and storage and retention of all personal data held.

The Charity may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the Local Authority, other schools and educational bodies, and potentially young person's services.

Everybody within the Charity is responsible for ensuring all company personnel comply with this policy and need to implement appropriate practices, processes, controls and training to ensure such compliance. Methods for keeping data secure are imperative, and the Charity believes that it is good practice to keep clear practical policies, backed up by written procedures where required.

The Charity expects all employees to work within the Charity's rules and procedures. All employees have a responsibility to conduct themselves in an appropriate and professional manner in accordance with the Code of Conduct and core values and co-operate in the application of this procedure.

This policy does not form part of any employee's contract of employment, and it may be amended at any time. The Charity may also vary this procedure, including any time limits, as appropriate in any case.

This policy should be read in conjunction with the following Charity policies:

- CCTV Policy
- Filtering & Monitoring Policy
- Acceptable use of Charity Internet, ICT Systems and Equipment Agreement: Staff Agency Workers, Trustees / Governors and applicable: Contractors, Volunteers & Visitors Agreement.
- Safeguarding Policy
- Talbot House Children's Charity Privacy Notice (Staff)

Data Protection Policy

1. Legislation and Guidance

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by [The Data Protection, Privacy and Electronic Communications \(Amendments etc\) \(EU Exit\) Regulations 2020](#).
- [Data Protection Act 2018 \(DPA 2018\)](#).
- It is based on guidance published by the Information Commissioner's Office (ICO) on the [UK GDPR](#) and guidance from the Department for Education (DfE) on [Generative artificial intelligence in education](#).
- It also reflects the ICO's guidance for the use of surveillance cameras and personal information.
- In addition, this policy complies with the Charity's **Memorandum and Articles of Association**.

2. Data Definitions

Term	Definition
Personal Data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: Name (including initials) Identification number Location data Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special Categories of Personal Data	Personal data which is more sensitive and so needs more protection, including information about an individual's: Racial or ethnic origin Political opinions Religious or philosophical beliefs Trade union membership Genetics Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes Health – physical or mental Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data Subject	The identified or identifiable individual whose personal data is held or processed.
Data Controller	A person or organisation that determines the purposes and the means of processing personal data.
Data Processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.

Data Protection Policy

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

3. The Data Controller

Our Charity processes personal data relating to parents / carers, pupils, employees and other relevant individuals, and therefore is a Data Controller.

- The Charity is registered with the ICO / has paid its data protection fee to the ICO, as legally required. (Delete as applicable.)

4. Roles and Responsibilities

This policy applies to all employees, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

- The Board of Trustees ("the Board") has:
 - Overall responsibility for ensuring that our Charity complies with all relevant data protection obligations.
- All staff (pending their individual job description) are responsible for:
 - Collecting, storing and processing any personal data in accordance with this policy.
 - Informing the Charity of any changes to their personal data, such as a change of address.
- Staff should contact a senior member of staff or the IT Support Assistant with any questions or queries, such as:
 - Queries relating to the operation of this policy, data protection law, retaining personal data or keeping personal data secure.
 - Any concerns that this policy is not being followed.
 - If they are unsure whether or not they have a lawful basis to use personal data in a particular way.
 - When they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK.
 - If there has been a data breach.
 - Whenever they are engaging in a new activity that may affect the privacy rights of individuals.
 - If they need help with any contracts or sharing personal data with third parties.
- Before sharing data, all staff members will ensure:
 - They are allowed to share it. We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:
 - There is an issue with a pupil or parent / carer that puts the safety of our staff at risk.
 - We need to liaise with other agencies – we will seek consent as necessary before doing this.
 - Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies.
 - That adequate security is in place to protect it.
 - Who will receive the data has been outlined in a privacy notice.
 - Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the Charity containing sensitive information must be supervised at all times.

Data Protection Policy

- The physical security of the Charity's buildings and storage systems, and access to them, is reviewed on a regular basis.
- The Charity takes its duties under the UK GDPR seriously and any unauthorised disclosure may result in disciplinary action. Continuity and recovery measures are in place to ensure the security of protected data.
- The Charity will share personal data with law enforcement and government bodies where we are legally required to do so.
- The Charity may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.
- Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

5. Data Protection Principles

All personal data obtained and held by the Charity will:

- Be processed fairly, lawfully and in a transparent manner.
- Be collected for specific, explicit, and legitimate purposes.
- Be adequate, relevant and limited to what is necessary for the purposes of processing.
- Be kept accurate and up to date. Every reasonable effort will be made to ensure that inaccurate data is rectified or erased without delay.
- Not be kept for longer than is necessary for its given purpose.
- Be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisational measures.
- Comply with the relevant data protection procedures for international transferring of personal data.

5.1 Personal data will be processed in recognition of an individuals' data protection rights, as follows:

- The right to be informed.
- The right of access.
- The right for any inaccuracies to be corrected (rectification).
- The right to have information deleted (erasure).
- The right to restrict the processing of the data.
- The right to portability.
- The right to object to the inclusion of any information.
- The right to regulate any automated decision-making and profiling of personal data.

6. Personal Data Protection Principles

Personal data is kept in personnel files or within the Charity's HR / payroll / school systems. The Charity will only process personal data where we have one (1) of six (6) 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the Charity can fulfil a contract with the individual, or the individual has asked the Charity to take specific steps before entering into a contract.
- The data needs to be processed so that the Charity can comply with a legal obligation.
- The data needs to be processed to ensure the vital interests of the individual or another person i.e. to protect someone's life.

Data Protection Policy

- The data needs to be processed so that the Charity can perform a task in the public interest or exercise its official authority.
- The data needs to be processed for the legitimate interests of the Charity (where the processing is not for any tasks the Charity performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden.
- The individual (or their parent / carer when appropriate in the case of a pupil) has freely given clear consent.

6.1 For special categories of personal data, we will also meet one (1) of the special category conditions for processing under data protection law:

- The individual (or their parent / carer when appropriate in the case of a pupil) has given explicit consent.
- The data needs to be processed to perform or exercise obligations or rights in relation to employment, social security or social protection law.
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent.
- The data has already been made manifestly public by the individual.
- The data needs to be processed for the establishment, exercise or defence of legal claims.
- The data needs to be processed for reasons of substantial public interest as defined in legislation.
- The data needs to be processed for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law.
- The data needs to be processed for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law.
- The data needs to be processed for archiving purposes, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest.

6.2 For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent / carer when appropriate in the case of a pupil) has given consent.
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent.
- The data has already been made manifestly public by the individual.
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights.
- The data needs to be processed for reasons of substantial public interest as defined in legislation.

6.3 Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

6.4 We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect or use personal data in ways which have unjustified adverse effects on them.

Data Protection Policy

- 6.5 Staff must only process personal data where it is necessary in order to do their jobs.
- 6.6 The Charity will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate. In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised.
- 6.7 The following types of data may be held by the Charity, as appropriate, on relevant individuals:
- Name, address, phone numbers - for individual and next of kin.
 - CVs and other information gathered during recruitment.
 - References from former employers.
 - National Insurance numbers.
 - Job title, job descriptions and pay grades.
 - Conduct issues such as letters of concern, disciplinary proceedings.
 - Holiday records.
 - Internal performance information.
 - Medical or health information.
 - Sickness absence records.
 - Tax codes.
 - Terms and conditions of employment.
 - Training details.
- Relevant individuals should refer to the Charity's **Privacy** Notice (Staff) for more information on the reasons for its processing activities, the lawful bases it relies on for the processing and data retention periods.

7. Individuals Other Rights and Subject Access Requests

Under data protection law, individuals have rights including:

Your right of access	You have the right to ask us for copies of your personal data.
Your right to rectification	You have the right to ask us to rectify personal data you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.
Your right to erasure	You have the right to ask us to erase your personal data in certain circumstances.
Your right to restriction of processing	You have the right to ask us to restrict the processing of your personal data in certain circumstances.
Your right to object to processing	You have the right to object to the processing of your personal data in certain circumstances.
Your right to data portability	You have the right to ask that we transfer the personal data you gave us to another organisation, or to you, in certain circumstances.
Your right to withdraw consent	When we use consent as our lawful basis you have the right to withdraw your consent.
Your right to challenge decisions based solely on automated decision making or profiling	Individuals have the right not to be subject to a decision when: • It is based on automated processing, e.g. profiling. • It produces a legal effect or a similarly significant effect on the individual.

Data Protection Policy

Be notified of a data breach	You have the right to be notified in the event of a data breach in certain circumstances.
Make a complaint to the ICO	You have the right to Make a complaint to the ICO.

- 7.1 Individuals have a right to make a 'subject access request' (SAR) to gain access to personal information that the Charity holds about them. This includes:
- Confirmation that their personal data is being processed.
 - Access to a copy of the data.
 - The purposes of the data processing.
 - The categories of personal data concerned.
 - Who the data has been, or will be, shared with.
 - How long the data will be stored for, or if this isn't possible, the criteria used to determine this period.
 - Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing.
 - The right to lodge a complaint with the ICO or another supervisory authority.
 - The source of the data, if not the individual.
 - Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.
 - The safeguards provided if the data is being transferred internationally.
- 7.2 Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:
- Name of individual.
 - Correspondence address.
 - Contact number and email address.
 - Details of the information requested.
- 7.3 If a SAR is received in any form staff must immediately forward it to the CEO.
- 7.4 If a request is made, the Charity has one (1) calendar month to respond. To make a data protection rights request, please contact us using the following details:
- Contact details:
Talbot House Children's Charity
Hexham Road
Walbottle
Newcastle upon Tyne
NE15 8HW
0191 229 0111
Email: office@talbothousecc.org.uk
- 7.5 Children and Subject Access Requests
Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must

Data Protection Policy

either be unable to understand their rights and the implications of a subject access request or have given their consent.

- Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.
- Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

7.6 Responding to subject access requests

When responding to requests, the Charity:

- May ask the individual to provide two (2) forms of identification.
- May contact the individual via phone to confirm the request was made.
- Will respond without delay and within one (1) month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant).
- Will provide the information free of charge.
- May tell the individual we will comply within three (3) months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within one (1) month, and explain why the extension is necessary.
- May not disclose information for a variety of reasons, such as if it:
 - Might cause serious harm to the physical or mental health of the pupil or another individual.
 - Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests.
 - Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it.
 - Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts.

7.7 If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

7.8 When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

8. Parental Requests to see Educational Records

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school term days of receipt of a written request.

- If the request is for a copy of the educational record, the Charity may charge a fee to cover the cost of supplying it.

Data Protection Policy

- This right applies as long as the pupil concerned is aged under 18.
- There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

9. Photographs and Videos

As part of our school activities, we may take photographs and record images of individuals within our school.

- We will obtain written consent from parents / carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and / or video will be used to both the parent / carer and the pupil.
- Any photographs and videos taken by parents / carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

9.1 Where photographs and videos are taken, uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns.
- Online on our website or social media pages.

9.2 Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

9.3 When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

9.4 The Charity has a comprehensive **CCTV Policy**; please refer to this document for further information regarding CCTV.

10. Artificial Intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents / carers may be familiar with generative chatbots such as ChatGPT and Google Bard etc.. The Charity recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

- To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.
- If personal and / or sensitive data is entered into an unauthorised generative AI tool, the Charity will treat this as a data breach and will follow the personal data breach procedure outlined in **Appendix 1**.

11. Data Security and Storage of Records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

Data Protection Policy

- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices (personal USB devices and / or external hard-drives are not permitted).
- Staff, are not usually permitted to store personal information on their personal devices are expected to follow the same security procedures as for Charity-owned equipment and any Charity information must be permanently deleted from any device, USB and / or external hard-drives upon leaving employment (confirmed by the IT Support Assistant).
- Please see our **Filtering & Monitoring Policy** and **Acceptable use of Charity Internet, ICT Systems and Equipment Agreement: Staff Agency Workers, Trustees / Governors and applicable: Contractors, Volunteers & Visitors Agreement**.
- The Charity reserves the right to access work email accounts and network drives if a member of staff is absent, e.g. sick leave or suspension, for the needs of the business only.

12. Data Retention and Disposal of Records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. For example, the Charity will:

- Securely shred or incinerate paper-based records, and overwrite or delete electronic files, using a third party to safely dispose of records on the Charity's behalf. The Charity requires any third party to provide sufficient guarantees that it complies with data protection law.
- Ensure that data is not kept for longer than is necessary.
- Education records may be kept for 75 years in line with current legislation if the file relates to child sexual abuse.

13. Personal Data Breaches

The Charity will make all reasonable endeavours to ensure that there are no personal data breaches.

- In the unlikely event of a suspected data breach, we will follow the procedure set out in **Appendix 1**.
- When appropriate, we will report the data breach to the ICO within 72-hours after becoming aware of it. Examples of breaches within our Charity context may include, but are not limited to:
 - A non-anonymised dataset being published on the website, which shows the exam results of pupils eligible for the pupil premium.
 - Safeguarding information being made available to an unauthorised person.
 - The theft of a laptop containing non-encrypted personal data about pupils.

14. Training

All staff are provided with data protection training as part of their induction process. The Head Teacher will ensure that data protection will also form part of continuing professional development, where changes to legislation, guidance or the Charity's / school's processes make it necessary.

15. Review

This policy is subject for review at any time, in line with recommended changes and may be subject for review prior to the date shown if deemed necessary, however, this policy is usually reviewed every two years. The HR Manager and IT Support Assistant will usually be responsible for reviewing this policy along with the Senior Manager Team.

Data Protection Policy

Appendix 1 – Personal Data Breach Procedure

This procedure is based on [guidance on personal data breaches](#) produced by the Information Commissioner's Office (ICO).

On finding or causing a breach or potential breach, the staff member / other must immediately notify the IT Support Assistant in person, by telephone or by email.

- A suitably appointed person will investigate the report and determine whether a breach has occurred. To decide, the appointed person will consider whether personal data has been accidentally or unlawfully:
 - Lost.
 - Stolen.
 - Destroyed.
 - Altered.
 - Disclosed or made available where it should not have been.
 - Made available to unauthorised people.
- Staff / others will co-operate with the investigation (including allowing access to information and responding to questions). This investigation will not be treated as a disciplinary investigation.
- If a breach has occurred or it is considered to be likely that is the case, the appointed person will alert the CEO.
- The appointed person and IT Support Assistant will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the appointed person and IT Support Assistant with this where necessary, and the IT Support Assistant should take external advice when required (e.g. from IT providers).
- The appointed person will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences.
- The appointed person will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's [self-assessment tool](#).
- The appointed person will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the Charity's computer system.
- Where the ICO must be notified, the appointed person will do this via the [‘report a breach’ page](#) of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the Charity's awareness of the breach. As required, the appointed person will set out a description of the nature of the personal data breach including, where possible:
 - The categories and approximate number of individuals concerned.
 - The categories and approximate number of personal data records concerned.
 - The name and contact details of the appointed person.
 - A description of the likely consequences of the personal data breach.
 - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual or individuals concerned.
- If all the above details are not yet known, the appointed person will report as much as they can within 72 hours of the Charity's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the appointed person expects

Data Protection Policy

- to have further information. The appointed person will submit the remaining information as soon as possible.
- Where the Charity is required to communicate with individuals whose personal data has been breached, the appointed person will tell them in writing. This notification will set out:
 - A description, in clear and plain language, of the nature of the personal data breach.
 - The name and contact details of the appointed person.
 - A description of the likely consequences of the personal data breach.
 - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual or individuals concerned.
 - The appointed person will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
 - The appointed person will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
 - Facts and cause.
 - Effects.
 - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals).
 - Records of all breaches will be stored on file and retained within the Administration Office (other secure Central storage area).
 - The appointed person, CEO, Head Teacher (if applicable), HR Manager (if applicable) and IT Support Assistant will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible following any investigation.
 - Details will be shared with the Chair of Trustees if / when deemed necessary, pending the seriousness of any data breach.

The CEO, Head Teacher and IT Support Assistant will meet periodically, as required, to assess recorded data breaches and identify any trends or patterns requiring action by the Charity to reduce risks of future breaches.

Actions to minimise the impact of data breaches

The Charity sets out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

- Members of staff who receive personal data sent in error must alert the sender, the IT Support Assistant as soon as they become aware of the error.
- Members of staff must attempt to recall the email as soon as they become aware of the error.
- If the sender is unavailable or cannot recall the email for any reason, the IT Support Assistant will attempt to recall it from external recipients and remove it from the email system (retaining a copy if required as evidence).

Data Protection Policy

- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the IT Support Assistant will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
- The IT Support Assistant will endeavour to obtain a written response from all the individuals who received the data, confirming that they have complied with this request.
- The IT Support Assistant will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.
- If safeguarding information is compromised, the IT Support Assistant will inform the CEO who is also a Designated Safeguarding Lead (DSL), and discuss whether the Charity should inform any, or all, of its safeguarding partners.

Sensitive information being disclosed via email (including safeguarding records)

If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.

The Charity will investigation and take action for any type of data breach, this may include, but are not limited to:

- Details of pupil premium interventions for named children being published on the website.
- Non-anonymised pupil exam results or staff pay information being shared with governors.
- A laptop containing non-encrypted sensitive personal data being stolen or hacked.
- Hardcopy reports sent to the wrong pupil or wrong families.

Data Protection Policy



I have read, understood and acknowledge this Policy and will endeavour to follow the guidance outlined within.

Print name: _____

Job Title: _____

Department: _____

Sign: _____

Date: _____

Please complete full details above, once complete please return to the HR Department within 5 working days.

Please do not hesitate to contact me should you have any questions.

HR Department

Talbot House Children's Charity