Data Protection

TRUST POLICY & PROCEDURE

Document Revised:	January 2022
Ratified by Trustees:	January 2022
Next Review Date:	August 2023

Content

The following sections are included in this policy document:

Statement of Intent

This Data Protection Policy sets out how Talbot House Trust (The Trust) handles the personal data of our employees, workers, agency staff, children, trustees and governors and other third parties.

The Trust is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the UK General Data Protection Regulation (UK GDPR).

The Trust 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.

This policy is in place to ensure all staff, Trustees and Governors (The Board) are aware of their responsibilities and outlines how the Trust complies with the following core data protection principles.

Everybody within the Trust 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.

Organisational methods for keeping data secure are imperative, and Talbot House Trust believes that it is good practice to keep clear practical policies, backed up by written procedures.

Talbot House Trust (North East) Limited ("the Trust") expects all employees to work within the Trusts rules and procedure. All employees have a responsibility to conduct themselves in an appropriate and professional manner in accordance with the Trust's Code of Conduct and Core Values, and co-operate in the application of this procedure.

This policy applies to all employees, trustees, workers, agency workers, self-employed contractors.

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

1. Legal framework

This policy has due regard to legislation, including, but not limited to the following:

- The UK General Data Protection Regulation (UK GDPR).
- The Freedom of Information Act 2000.
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016).
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004.
- The School Standards and Framework Act 1998.

This policy will also have regard to the following guidance:

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'.
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'.

This policy will be implemented in conjunction with the following other Trust policies:

- **CCTV Policy**.
- **Gate Entry and Visitors Management Policy**.

2. Applicable data

For the purpose of this policy, personal data refers to information that relates to an identifiable, living, individual, including information such as online identifier, e.g. an IP address. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

Sensitive personal data is referred to in the UK GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data and data concerning health matters.

3. Personal data protection principles

In accordance with the requirements outlined in the UK GDPR, personal data will be:

Processed lawfully, fairly and in a transparent manner in relation to individuals

Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals.

Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The UK GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the data protection principles", which are listed above.

4. Accountability

Talbot House Trust will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the UK GDPR.

The Trust will provide comprehensive, clear and transparent privacy policies.

Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or that in relation to criminal convictions and offences.

Internal records of processing activities will include the following:

- Name and details of the organisation.
- Purpose(s) of the processing.
- Description of the categories of individuals and personal data.
- Retention schedules.
- Categories of recipients of personal data.
- Description of technical and organisational security measures.
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place.

The Trust will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Data minimisation;
- Pseudonymisation;
- Transparency;
- Allowing individuals to monitor processing;
- Continuously creating and improving security features;
- Data protection impact assessments will be used, where appropriate.

5. Lawful processing

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

The Trust may only collect, process and share personal data fairly and lawfully and for specified reasons. The UK GDPR restricts our actions regarding personal data to specified lawful purposes. These restrictions are not intended to prevent processing, but to ensure that we process personal data fairly and without adversely affecting the data subject.

The legal basis for processing data will be identified and documented prior to data being processed.

The Trust will act as a data processor; however, this role may also be undertaken by other third parties.

Under the UK GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained.

Processing is necessary for:

- Compliance with a legal obligation.
- The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- For the performance of a contract with the data subject or to take steps to enter into a contract.
- Protecting the vital interests of a data subject or another person.
- For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (This condition is not available to processing undertaken by the Trust in the performance of its tasks).

Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State Law.
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
- Processing relates to personal data manifestly made public by the data subject.

Processing is necessary for:

- Carrying out obligations under employment, social security or social protection law, or a collective agreement.
- Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.

- The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
- Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards.
- The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.
- Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
- Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

6. Consent

Consent will be sought prior to processing any data, which cannot be done so under any other lawful basis, such as complying with a regulatory requirement.

Consent must be a positive indication. It **cannot** be inferred from silence, inactivity or pre-ticked boxes.

Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

Where consent is given, a record will be kept documenting how and when consent was given.

The Trust ensures that consent mechanisms meet the standards of the UK GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

Consent accepted under the DPA will be reviewed to ensure it meets the standards of the UK GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

Consent can be withdrawn by the individual at any time.

Where a young person is under the age of 16, the consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a young person.

When gaining consent from a young person, consideration will be given to the age, maturity and mental capacity of the young person in question. Consent will only be gained from young people where it is deemed that they have a sound understanding of what they are consenting to.

7. The right to be informed

The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language, which is concise, transparent, easily accessible and free of charge.

If services are offered directly to a young person, the Trust will ensure that the privacy notice is written in a clear, plain manner that the young person will understand.

In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The contact details of the controller (the Trust), and where applicable, the controller's representative.
- The purpose of, and the legal basis for, processing the data.
- The legitimate interests of the controller or third party.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to third countries and the safeguards in place.
- The retention period of criteria used to determine the retention period.

The existence of the data subject's rights, including the right to:

- Withdraw consent at any time.
- Lodge a complaint with a supervisory authority.
- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.
- Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided.
- Where data is not obtained directly from the data subject, information regarding the categories of personal data that the Trust holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.
- For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

In relation to data that is not obtained directly from the data subject, this information will be supplied:

- Within one month of having obtained the data.
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed;
- If the data are used to communicate with the individual, at the latest when the first communication takes place.

8. The right of access

Individuals have the right to obtain confirmation that their data is being processed.

Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

The Trust will verify the identity of the person making the request before any information is supplied.

A copy of the information will be supplied to the individual free of charge; however, the Trust may impose a 'reasonable fee' to comply with requests for further copies of the same information.

Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

All fees will be based on the administrative cost of providing the information.

All requests will be responded to without delay and at the latest, within one month of receipt.

In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

Where a request is manifestly unfounded or excessive, the Trust holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

In the event that a large quantity of information is being processed about an individual, the Trust will ask the individual to specify the information the request is in relation to.

9. The right to rectification

Individuals are entitled to have any inaccurate or incomplete personal data rectified.

Where the personal data in question has been disclosed to third parties, the Trust will inform them of the rectification where possible.

Where appropriate. The Trust will inform the individual about the third parties that the data has been disclosed to.

Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

Where no action is being taken in response to a request for rectification, the Trust will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

10. The right to erasure

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws their consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.

- The personal data was unlawfully processed.
- The personal data is required to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a young person.

The Trust has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information.
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- For public health purposes in the public interest.
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes.
- The exercise or defence of legal claims.
- As a young person may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a young person has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

Where personal data has been made public within an online environment, the Trust will inform other organisations who process the personal data to erase links to and copies to the personal data in question.

11. The right to restrict processing

Individuals have the right to block or suppress the Trust's processing of personal data.

In the event that processing is restricted, the Trust will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

The Trust will restrict the processing of personal data in the following circumstances:

- Where the individual contests the accuracy of the personal data, processing will be restricted until the Trust has verified the accuracy of the data.
- Where an individual has objected to the processing and the Trust is considering whether their legitimate grounds override those of the individual.
- Where processing is unlawful and the individual opposes erasure and requests restriction instead.
- Where the Trust no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.
- If the personal data in question has been disclosed to third parties, the Trust will inform them about the restriction on the personal data, unless it is impossible or involves disproportionate effort to do so.
- The Trust will inform individuals when a restriction on processing has been lifted.

12. The Right to Data Portability

Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller.
- Where the processing is based on the individuals consent or for the performance of a contract.
- When processing is carried out by automated means.
- Personal data will be provided in a structured, commonly used and machine-readable form.
- The Trust will provide the information free of charge.
- Where feasible, data will be transmitted directly to another organisation at the request of the individual.
- The Trust is not required to adopt or maintain processing systems which are technically compatible with other organisations.
- In the event that personal data concerns more than one individual, the Trust will consider whether providing the information would prejudice the rights of any other individual.
- The Trust will respond to any requests for portability within one month.
- Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

Where no action is being taken in response to a request, the Trust will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

13. The right to object

The Trust will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest.
- Direct marketing.
- Processing for purposes of scientific or historical research and statistics.

Where personal data is processed or the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.

- The Trust will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, were the Trust can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

Where personal data is processed for direct marketing purposes:

- The Trust will stop processing personal data for direct marketing purposes as soon as soon as an objection is received.
- The Trust cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the Trust is not required to comply with an objection to the processing of the data.
- Where the processing activity is outlined above, but is carried out online, the Trust will offer a method for individuals to object online.

14. Automated decision making and 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.
- The Trust will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

When automatically processing personal data for profiling purposes, the Trust will ensure that the appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.

Using appropriate mathematical or statistical procedures.

Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.

Securing personal data in a way that is proportionate to the risks to the interests and rights of the individual and prevents discrimination

Automated decisions must not concern a young person or be based on the processing of sensitive data, unless:

- The Trust has the explicit consent of the individual.

- The processing is necessary for reasons of substantial public interest on the basis of Union/Member State law.

15. Privacy by design and privacy impact assessments

The Trust will act in accordance with the UK GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the Trust has considered and integrated data protection into processing activities.

Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the Trust's data protection obligations and meeting individual's expectations of privacy.

DPIA's will allow the Trust to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the Trust's reputation which might otherwise occur.

A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

A DPIA will be used for more than one project, where necessary.

High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling.
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences.
- The use of CCTV.

The Trust will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes;
- An assessment of the necessity and proportionality of the processing in relation to the purpose;
- An outline of the risks to individuals;
- The measures implemented in order to address risk.

Where a DPIA indicates high risk data processing, the Trust will consult the ICO to seek its opinion as to whether the processing operation complies with the UK GDPR.

16. Data breaches

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The Head Teacher will ensure that all school staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

All notifiable breaches will be reported to the relevant supervisory authority with 72 hours of the Trust becoming aware of it.

The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.

In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the Trust will notify those concerned directly.

A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

In the event that a breach is sufficiently serious, the public will be notified without undue delay.

Effective and robust breach detection, investigation and internal reporting procedures are in place at the Trust, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned.
- An explanation of the likely consequences of the personal data breach.
- A description of the proposed measures to be taken to deal with the personal data breach.
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects.
- Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

17. Data security & confidentiality

Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

Confidential paper records will not be left unattended or in clear view anywhere with general access.

Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.

Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.

All electronic devices are password-protected to protect the information on the device in case of theft.

Where possible, the Trust enables electronic devices to allow the remote blocking or deletion of data in case of theft.

Staff and governors will not use their personal laptops or computers for Trust purposes unless they have express permission from the CEO.

All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.

Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. Keeping devices under lock and key. The person taking the information from the premises accepts full responsibility for the security of the data.

Before sharing data, all staff members will ensure:

- They are allowed to share it.
- 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 Trust containing sensitive information are supervised at all times.
- The physical security of the Trust's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be out in place.
- Talbot House Trust 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.

18. Publication of information

Talbot House Trust publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

- Policies and Procedures.
- Minutes of meetings.
- Annual reports.
- Financial information.
- Classes of information specified in the publication scheme are made available quickly and easily on request.
- The Trust will not publish any personal information, including photos, on its website without the permission of the effect individual.
- When uploading information to the Trust's website, staff are considerate of any metadata or deletions, which could be accessed in documents and images on the site.

19. CCTV and photography

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

Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the UK GDPR.

20. Access to information

20.1 The Trust 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.

21. Data retention

Data will not be kept for longer than is necessary.

Unrequired data will be deleted as soon as practicable.

Education and residential records must be kept for 75 years in line with current legislation.

Some educational records relating to former young people or employees of the Trust may be kept for an extended period for legal reasons.

Paper copies will be shredded and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

22. DBS data

All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

Data provided by the DBS will never usually be duplicated, although photocopies can be retained as part of the on boarding processing for a period of up to 6 months.

Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibility as a data handler.

If you believe that the Trust has not complied with your data protection rights, you can complain to the Information Commissioner, they can be contacted at:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Telephone: 0303 123 1113 (local rate) or 01625 545 745 (national rate).

23. Review

This policy is non-contractual and is subject for review in line with changes to legislation.

This policy may be subject for review prior to the date shown if deemed necessary.

The SMT and HR Department will be responsible for reviewing this policy.

Appendix 1 - Interpretation

Definitions:

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The UK GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

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. Profiling is an example of Automated Processing.

Company Personnel: all employees, workers, agency workers, children and others.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

UK General Data Protection Regulation (UK GDPR): the retained EU law version of the General Data Protection Regulation ((EU) 2016/679). Personal Data is subject to the legal safeguards specified in the UK GDPR.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive Personal 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 Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the UK GDPR.

Privacy Guidelines: the Company privacy and UK GDPR related guidelines provided to assist in interpreting and implementing this Policy and related policies.

Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when the Company collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing 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.

Related Policies: the Company's policies, operating procedures or processes related to this Privacy Standard and designed to protect Personal Data.

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

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 Trust