Data Protection Policy

Policy Name:	Data Protection Policy
Version:	1
Date published:	23/09/2024
Date to be reviewed by:	September 2025
Role of Reviewer:	HR Manager/ Data Protection Officer
Statutory (Y/N):	N
Published on website: *	3C
Policy Level: **	1
Relevant to:	All Staff
Produced in consultation with:	N/A
Approved by:	18/09/2024
Approval date:	Care & Operations Committee

*Publication on website			
Alliance website		School website	
1	Statutory publication	A	Statutory publication
2	Good practice	B	Good practice
3	Not required	C	Not required

**Policy level			
1	Trust wide	Single policy relevant to everyone and consistently applied across all schools and departments, with no variation. e.g. Complaints procedure	Statutory policies approved by the Alliance Board of Trustees (or designated Trustee Committee). Non-statutory policies approved by the CEO with exception of Executive Pay.
2	Trust core values	This policy defines the Trust core values in the form of a Trust statement to be incorporated fully into all other policies on this subject, that in addition contain relevant information, procedures and or processes contextualised to that school. e.g. Safeguarding, Behaviour	Statements in statutory policies approved by the Alliance Board of Trustees (or designated Trustee Committee). Statements in non-statutory policies approved by the CEO. Policy approved by Local School Board.
3	School/department	These policies/procedures are defined independently by schools as appropriate. E.g. Anti-bullying	Approved by Local School Board.

Contents

SECTION A GENERAL OVERVIEW

1 Introduction

1.1 This Policy sets out the obligations of The Alliance regarding data protection and the rights of, pupils, parents, staff and visitors ("data subjects") in respect of their personal data under the Data Protection Act 2018 and the associated UK GDPR.

1.2 The UK GDPR defines "personal data" as any information relating to an identified or identifiable natural person (a "data subject"). A person may be identified by: name, identification number, location data, an online identifier, factors specific to the physical, genetic, mental, economic, cultural, or social identity of that person.

1.3 This Policy sets out the Trust's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles must be followed at all times by the Trust, its employees, agents, contractors, or other parties working on behalf of the Trust.

1.4 The Trust places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals.

1.5 A data subject is the identifiable living individual to whom personal data relates.

1.6 A data processor is a person, public authority, agency or other body which processes personal data on behalf of the controller. Processors act on behalf of the controller and under their authority. An example of this would be a payroll processing company.

1.7 A data controller in this context is The Alliance.

2 The Data Protection Principles

2.1 This Policy aims to ensure compliance with the UK GDPR. The UK GDPR sets out the following principles with which any party handling personal data must comply. All personal data must be:

2.1.1 Processed lawfully, fairly, and in a transparent manner in relation to the data subject.

2.1.2 Collected for specified, explicit, and legitimate purposes and not further processed for different purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes are considered legitimate purposes.

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

2.1.4 Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified without delay.

2.1.5 Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed purposes.

2.1.6 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.

3 Organisational Measures

3.1 The Trust shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

3.2 All employees, agents, contractors, or other parties working on behalf of The Trust shall be made fully aware of both their individual responsibilities and our responsibilities under the UK GDPR and under this Policy, and shall have free access to a copy of this Policy;

3.3 Only employees, agents, sub-contractors, or other parties working on behalf of the Trust that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Trust;

3.4 All employees, agents, contractors, or other parties working on behalf of the Trust handling personal data will be appropriately trained to do so;

3.5 All employees, agents, contractors, or other parties working on behalf of the Trust handling personal data will be appropriately supervised;

3.6 All employees, agents, contractors, or other parties working on behalf of the Trust handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;

3.7 Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

3.8 All personal data held by the Trust shall be reviewed periodically, as set out in the Trust's Data Retention Policy;

3.9 The contravention of these rules will be treated as a disciplinary matter.

3.10 All employees, agents, contractors, or other parties working on behalf of the Trust handling personal data will be bound to do so in accordance with the principles of the UK GDPR and this Policy

3.11 All agents, contractors, or other parties working on behalf of the Trust handling personal data must ensure that employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Trust arising out of this Policy and the UK GDPR; and

3.12 Where any agent, contractor or other party working on behalf of the Trust handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Trust against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

4 Data Protection Impact Assessments

4.1 The Trust shall carry out Data Protection Impact Assessments for new projects and/or new uses of personal data which are likely to result in a high risk to the rights and freedoms of data subjects under the UK GDPR.

4.2 Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:

4.2.1 The type(s) of personal data that will be collected, held, and processed.

4.2.2 The purpose(s) for which personal data is to be used;

4.2.3 The Trust's objectives;

4.2.4 How personal data is to be used;

4.2.5 The parties (internal and/or external) who are to be consulted;

4.2.6 The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;

4.2.7 Risks posed to data subjects;

4.2.8 Risks posed both within and to the Trust; and

4.2.9 Proposed measures to minimise and handle identified risks.

5 Data Breach Notification

5.1 All personal data breaches must be reported immediately to the Trust via the Data Protection Lead at each school who will report it to the Data Protection Officer. If you are unsure who your relevant Data Protection Lead is, please contact the Head's PA.

5.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

5.3 In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

5.4 Data breach notifications shall include the following information:

5.4.1 The categories and approximate number of data subjects concerned;

5.4.2 The categories and approximate number of personal data records concerned;

5.4.3 The name and contact details of the Trust's data protection officer (or other contact point where more information can be obtained);

5.4.4 The likely consequences of the breach;

5.4.5 Details of the measures taken, or proposed to be taken, by the Trust to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

SECTION B PROCESSING DATA

1 Specified, Explicit, and Legitimate Purposes

1.1 The Trust collects and processes the personal data set out in our Privacy Notices. This includes:

1.1.1 Personal data collected directly from data subjects; and

1.1.2 Personal data obtained from third parties.

1.2 The Trust only collects, processes, and holds personal data for the specific purposes set out in Section E Appendix 1 of this Policy (or for other purposes expressly permitted by the UK GDPR).

1.3 Data subjects are kept informed at all times of the purpose or purposes for which the Trust uses their personal data. Please refer to Section C for more information on keeping data subjects informed.

2 Accuracy of Data and Keeping Data Up to Date

2.1 The Trust shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Section C, below.

2.2 The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

3 Data Retention

3.1 The Trust shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

3.2 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

3.3 For full details of the Trust's approach to data retention, including retention periods for specific personal data types held by the us, please refer to our Data Retention Policy which is available on request.

4 Secure Processing

The Trust shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided in Section D of this Policy.

5 Accountability and Record-Keeping

5.1 The Trust's Data Protection Officer is Sarah Horrigan – HRBP: ER/IR.

5.2 The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Trust's other data protection-related policies, and with the UK GDPR and other applicable data protection legislation.

5.3 The Trust shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

5.3.1 The name and details of The Trust, its Data Protection Officer, and any applicable third-party data processors;

5.3.2 The purposes for which The Trust collects, holds, and processes personal data;

5.3.3 Details of the categories of personal data collected, held, and processed by The Trust, and the categories of data subject to which that personal data relates;

5.3.4 Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;

5.3.5 Details of how long personal data will be retained by the Trust (please refer to our Data Retention Policy); and

5.3.6 Detailed descriptions of all technical and organisational measures taken by the Trust to ensure the security of personal data.

6 Data Portability

6.1 The Trust processes personal data using automated means.

6.2 Data subjects have a right to to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers).

6.3 All requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed.

7 Transferring Personal Data to a Country without an adequacy decision

7.1 The Trust may from time to time transfer ('transfer' includes making available remotely) personal data to countries without a suitable adequacy decision from the UK Government.

7.2 The transfer of personal data to a country without an adequacy decision shall take place only if one or more of the following applies:

7.2.1 The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the UK Government has determined ensures an adequate level of protection for personal data;

7.2.2 The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the UK Government compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the UK GDPR); contractual clauses agreed and authorised by the competent supervisory authority;

7.2.3 The transfer is made with the informed consent of the relevant data subject(s);

7.2.4 The transfer is necessary for the performance of a contract between the data subject and the Trust (or for pre-contractual steps taken at the request of the data subject);

7.2.5 The transfer is necessary for important public interest reasons;

7.2.6 The transfer is necessary for the conduct of legal claims;

7.2.7 The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or

7.2.8 The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

SECTION C INDIVIDUAL RIGHTS

1 The Rights of Data Subjects

1.1 The Data Protection Act 2018 and the UK GDPR sets out the following rights applicable to data subjects (please refer to the parts of this policy indicated for further details):

1.1.1 The right to be informed

1.1.2 The right of access

1.1.3 The right to rectification

1.1.4 The right to erasure (also known as the 'right to be forgotten')

1.1.5 The right to restrict processing

1.1.6 The right to data portability

1.1.7 The right to object and

1.1.8 Rights with respect to automated decision-making and profiling.

2 Keeping Data Subjects Informed

2.1 The Trust shall inform the data subject of the purpose of collecting data.

2.2 Usual practice shall be to inform the data subject at the point of collection, however, in exceptional circumstances this may be at the point of first communication or prior to the data being transferred to a third party.

2.3 The following information shall be provided:

2.3.1 Details of the Trust including, but not limited to, the identity of its Data Protection Officer;

2.3.2 The purpose(s) for which the personal data is being collected and will be processed (as detailed in Section B of this Policy) and the legal basis justifying that collection and processing;

2.3.3 Where applicable, the legitimate interests upon which the Trust is justifying its collection and processing of the personal data;

2.3.4 The categories of personal data collected and processed;

2.3.5 Where the personal data is to be transferred to one or more third parties, details of those parties;

2.3.6 Details of data retention;

2.3.7 Details of the data subject's rights under the UK GDPR;

2.3.8 Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it.

3 Data Subject Access

3.1 Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the Trust holds about them, what it is doing with that personal data, and why.

3.2 Employees wishing to make a SAR should contact Human Resources.

3.3 Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

3.4 Responses to SARs shall be dependent upon the terms of the UK GDPR, the Data Protection Act (2018) and associated ICO guidance.

3.5 The Trust does not charge a fee for the handling of normal SARs. The Trust reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

4 Rectification of Personal Data

4.1 Data subjects may have the right to require the Trust to rectify any of their personal data that is inaccurate or incomplete. The Trust shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

4.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

5 Erasure of Personal Data

5.1 Data subjects have the right to request that the Trust erases the personal data it holds about them in the following circumstances:

5.1.1 It is no longer necessary for The Trust to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;

5.1.2 The data subject wishes to withdraw their consent to The Trust holding and processing their personal data;

5.1.3 The data subject objects to The Trust holding and processing their personal data (and there is no overriding legitimate interest to allow the Trust to continue doing so) (see Part 18 of this Policy for further details concerning the right to object);

5.1.4 The personal data has been processed unlawfully;

5.1.5 The personal data needs to be erased in order for The Trust to comply with a particular legal obligation; or

5.1.6 The personal data is being held and processed for the purpose of providing information society services to a child.

5.2 Unless the Trust has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

5.3 In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

6 Restriction of Personal Data Processing

6.1 Data subjects may request that the Trust restricts processing the personal data it holds about them. If a data subject makes such a request, The Trust shall in so far as is possible ensure that the personal data is only stored and not processed in any other fashion.

6.2 If the Trust is required to process the data for statutory purposes or for reasons of legal compliance, then the Trust shall inform the Data Subject that this processing is expected to take place. If possible, this notice will be provided prior to processing.

6.3 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

7 Objections to Personal Data Processing

7.1 Data subjects have the right to object to the Trust processing their personal data based on performing a task in the public interest. Its' legitimate interests, or direct marketing (including profiling)

7.2 Where a data subject objects to the Trust processing their personal data, the Trust shall cease such processing immediately, unless it can be demonstrated that the Trust's grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for legal claims.

7.3 Where a data subject objects to the Trust processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the UK GDPR, "demonstrate grounds relating to their particular situation". The Trust is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

8 Profiling

8.1 The Trust uses personal data for profiling purposes. These purposes relate to helping students maximise achievement and monitor staff performance.

8.2 When personal data is used for profiling purposes, the following shall apply:

8.2.1 Clear information explaining the profiling shall be provided to data subjects, including the significance and likely consequences of the profiling;

8.2.2 Appropriate mathematical or statistical procedures shall be used;

8.2.3 Technical and organisational measures shall be implemented to minimise the risk of errors. If errors occur, such measures must enable them to be easily corrected; and

8.2.4 All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling.

9 Personal Data Collected, Held, and Processed

The Trust uses a wide range of personal data across many processes. More detail can be found in our privacy notices. If you wish to view the complete lists of categories of personal data we process please contact our Data Protection Officer.

SECTION D DATA SECURITY

1 Transferring Personal Data and Communications

1.1 The Trust shall ensure that the appropriate measures are taken with respect to all communications and transfers involving personal data:

1.1.1 Personal data may be transmitted over secure networks only.

1.1.2 The Trust will ensure that where special category personal data or other sensitive information is sent in the post so that it shall be possible to demonstrate that it was delivered.

1.1.3 Where special category personal data or other sensitive information is to be sent by e-mail the email will either be sent using a suitable encryption method or the data will be sent in an attached, encrypted document.

1.1.4 Where personal data is to be transferred in removal storage devices (USB sticks), these devices shall be encrypted. The use of unencrypted removable storage devices is prohibited by The Trust.

2 Storage

2.1 The Trust shall ensure that the following measures are taken with respect to the storage of personal data:

2.1.1 All electronic copies of personal data should be stored securely using passwords or user access rights and where appropriate data encryption;

2.1.2 All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;

2.1.3 All personal data relating to the operations of The Trust, stored electronically, should be backed up on a regular basis

2.1.4 Where any member of staff stores personal data on a mobile device (whether that be computer, tablet, phone or any other device) then that member of staff must abide by the Acceptable Use policy of the Trust.

3 Disposal

3.1 When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to the Trust's Data Retention Policy.

4 Use of Personal Data

4.1 The Trust shall ensure that the following measures are taken with respect to the use of personal data:

4.1.1 No personal data may be shared informally and if anyone requires access to any personal data that they do not already have access to, this must be requested from the Data Protection Officer

4.1.2 No personal data may be transferred without the initial authorisation of the Data Protection Officer.

4.1.3 Personal data must be handled with care at all times and should not be left unattended or on view.

4.1.4 If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it; and

4.1.5 Where personal data held by each school is used for marketing purposes, it shall be the responsibility of the Headteacher/ Head of School to ensure that the appropriate consent is obtained.

5 IT Security

5.1 The Trust shall ensure that the following measures are taken with respect to IT and information security:

5.1.1 The Trust requires that any passwords used to access personal data shall have a minimum of 8 characters, composed of a mixture of upper- and lower-case characters and numbers. Passwords are not expected to be changed upon a regular basis but users will be expected to change their password if instructed by The Trust.

5.1.2 Under no circumstances should any passwords be written down or shared, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;

5.1.3 The Trust's IT staff shall be responsible for installing any and all security-related updates as soon as reasonably and practically possible, unless there are valid technical reasons not to do so; and

5.1.4 No software may be installed on any Company-owned computer or device without the prior approval of the IT Manager.

5.1.5 Where members of staff or other user use online applications that require the use of personal data, the use of that application must be signed off by the IT Manager.

SECTION E

1 APPENDIX 1 - Lawful, Fair, and Transparent Data Processing

1.1 The UK GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The UK GDPR states that processing of personal data shall be lawful if at least one of the following applies:

1.1.1 The data subject has given consent to the processing of their personal data for one or more specific purposes.

1.1.2 The processing is necessary for the performance of a contract involving the data subject or to take steps at the request of the data subject prior to entering into a contract with them.

1.1.3 The processing is necessary for compliance with a legal obligation.

1.1.4 The processing is necessary to protect the vital interests of the data subject or of another person.

1.1.5 The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority; or

1.1.6 The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

1.2 If the personal data in question is “special category data” (e.g. data concerning the subject’s: race, ethnicity, politics, religion, trade union membership, genetics, biometrics, health, sex life, or sexual orientation), at least one of the following conditions must be met:

1.2.1 The data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless UK law prohibits them from doing so).

1.2.2 The processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent.

1.2.3 The data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities. The data subject must be a member or former member that has regular contact with the body.

1.2.4 The processing relates to personal data which is clearly made public by the data subject.

1.2.5 The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity.

1.2.6 The processing is necessary for substantial public interest reasons, on the basis of UK law which shall be proportionate to the aim pursued. E.g. the controller cannot request full medical history if only confirmation of a disability is required.

1.2.7 The processing is necessary for the purposes of medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of UK law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the UK GDPR.

1.2.8 The processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health, on the basis of UK law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or

1.2.9 The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the UK GDPR based on UK law which shall be proportionate to the aim pursued and provide for suitable and specific measures to safeguard the rights and the interests of the data subject.