Aldridge Education
Data Protection Policy

Policy Title:	Aldridge Education Data Protection Policy
Version:	May 2018
Trust Board Approval:	May 2018
Date of Next Review:	August 2019

Aldridge Education
Data Protection Policy

1. Background

Aldridge Education and its academies collect and use personal information about staff, students, parents and other individuals in order to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the Trust and its academies comply with statutory obligations.

The named people with overall responsibility for personal data within Aldridge Education are the Trust CEO and Director of Governance and HR. The Principal and academy Finance Director are responsible for academy operation of this policy.

Aldridge Education is registered, as a Data Controller, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website. All schools also have a duty to issue a Privacy Notice to all students and parents; this summarises the information held on students, why it is held and the other parties with whom it may be shared.

2. Aims & Objectives

The aim of this policy is to provide a model set of guidelines to enable Aldridge Education staff, parents and students to understand:

- The law regarding personal data
- How staff, parents and students can access personal data

The objective of the policy is to ensure that Aldridge Education and its academies act within the requirements of the Data Protection Act 1998, the General Data Protection Regulation Act 2018 other related legislation when retaining and storing personal data, and when making it available to individuals, and that the process of responding to enquiries for other information is also legal under the Freedom of Information Act 2000 (in force from 1st January 2005).

3. What is Personal Information?

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held. Examples of this would be contact details, students' education records or photographs taken at academy events.

4. Data Protection Principles

There are a number of enforceable principles that must be adhered to at all times:

- Personal data shall be processed fairly, lawfully and in a transparent manner
- Personal data shall be collected only for one or more specified and lawful purposes and processed in a way that is compatible with those purposes
- Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Personal data shall be accurate and where necessary, kept up to date and every reasonable step should be taken to delete or rectify inaccurate data without delay
- Personal data should be kept in a form which permits identification of data subjects for no longer than is necessary; personal data may be stored for longer if this is solely for archiving purposes in

the public interest, scientific, historical, research or statistical purposes subject to appropriate measures to safeguard the rights of individuals
- Personal data shall be processed in a way that ensures appropriate security of the personal data, including protection against accidental loss, destruction or damage

5. Policy Statement

Aldridge Education and its academies are committed to maintaining the above principles at all times. Therefore we will:

- Inform individuals why information is being collected when it is collected.
- Inform individuals when their information is shared, and why and with whom it was shared.
- Check the quality and the accuracy of the information it holds.
- Ensure that information is not retained for longer than is necessary.
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely.
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.
- Share information with others only when it is legally appropriate to do so.
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests.
- Ensure our staff are aware of and understand our policies and procedures.

6. Lawful Processing

We collect and use student information under Article 6, and Article 9 of the GDPR where data processed is a special category data and for data collection purposes under the Education Act 1996 https://www.gov.uk/education/data-collection-and-censuses-for-schools

The lawful bases for processing are set out in Article 6 of the GDPR. One of these must apply whenever we process personal data:

(a) Consent: the individual has given clear consent for us to process your personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract we have with you, or because you have asked us to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for us to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect an individual's personal data which overrides those legitimate interests. (This does not apply to schools who are a public authority and the processing of data is required to perform official tasks.)

7. Privacy Notices and the right to be informed

A privacy notice is a statement that describes how we use, retain and disclose personal information. Different organisations sometimes use different terms and it can be referred to as a privacy statement, a fair processing notice or a privacy policy.

To ensure that we process your personal data fairly and lawfully we are required to inform you:

- What information we collect, hold and share.
- Why we collect and use this information
- The lawful basis on which we use this information.
- Who we share this information with.
- Why we share this information.
- Our data collection requirements.
- How you can access this data and your rights.

Copies of our privacy notices are at appendix A and can also be found on the website.

8. Consent

Where consent is required this must be a positive action and it cannot be inferred from silence, inactivity or pre-ticked boxes. Consent forms are provided to students over the age of 12, parents and staff and a record will be kept of what consent was given and when.

Consent that has been given under the Data Protection Act 1998 that fully meets the requirement of the GDPR will be retained.

You may withdraw your consent at any time by notifying Will Ames on 01254 819500, alternatively email will.ames@daca.uk.com or the Trust at info@aldridgeeducation.org

9. Right of access

Individuals have the right to obtain confirmation that their data is being processed and to have access to the personal data in order to verify that the processing is lawful. This is known as a Subject Access Request. Details of how to make a Subject Access Request are in section xx

10. The right to rectification

Individuals are entitled to have any inaccurate or incomplete personal data rectified. We will also take the following action:

- Where the personal data in question has been disclosed to third parties, we will inform them of the rectification where possible
- Where appropriate, we will inform the individual about the third parties that the data has been disclosed to
- Requests for rectification will completed within one month; this may 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, we will explain the reason for this and will inform you or your right to complain to the Trust or the Information Commissioner.

11. 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 consent has been withdrawn
- When an 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 child

We have 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 of the Academy or Trust
- 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 child 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 child has given consent to processing and they later request erasure of the data, regardless of their 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, we will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

12. The right to restrict processing

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

In the event that processing is restricted, we 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.

We will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until we have verified the accuracy of the data
- Where an individual has objected to the processing and we are considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restriction instead
- Where we 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, we will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

We will inform individuals when a restriction on processing has been lifted.

13. 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 us
- Where the processing is based on the individual's 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. We will provide the information free of charge.

Where feasible, data will be transmitted directly to another organisation at the request of the individual but we are not required to adopt or maintain processing systems which are technically compatible with other organisations.

In the event that the personal data concerns more than one individual, we will consider whether providing the information would prejudice the rights of any other individual.

We will respond to any requests for portability within one month.

Where the request is complex, or a number of requests have been received, the time frame 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, we 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 Trust or Information Commissioner.

14. The right to object

We will inform individuals of their right to object and this is outlined in the privacy notice.

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 for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to their particular situation
- We will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual

- We will stop processing personal data for direct marketing purposes as soon as an objection is received
- We 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 Academy is not required to comply with an objection to the processing of the data.

15. Privacy by design and privacy impact assessments

We will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how we have 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 our data protection obligations and meeting individuals' expectations of privacy.

DPIAs will allow us to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the our reputation which might otherwise occur. A DPIA will be used 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

We 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, we will consult the ICO to seek its opinion as to whether the processing operation complies with the 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.

All staff members will be made aware of, and understand, what constitutes as a data breach as part of their induction and ongoing training.

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the Information

Commissioner will be informed with all notifiable breaches reported within 72 hours of the Academy or Trust becoming aware of it.

In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, we will notify those concerned directly as soon as reasonably possible after becoming aware of the data breach.

Effective and robust breach detection, investigation and internal reporting procedures are in place across the Trust, which aid decision making in relation to who should be notified of a breach.

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
- The name and contact details of the Data Protection Officer
- 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

17. Data security

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

Staff will not use their personal laptops, computers or mobile phones to store the data of students, parents or other members of staff.

All 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.

When sending confidential information by fax, staff will always check that the recipient is correct before sending.

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 Trust 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 containing sensitive information are supervised at all times.

The physical security of 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 put in place.

The Data Protection Officer is responsible for continuity and recovery measures are in place to ensure the security of protected data.

18. Publication of information

We publish a publication scheme on our website outlining classes of information that will be made routinely available, including:

- Policies and procedures
- Annual reports
- Financial information

Classes of information specified in the publication scheme are made available quickly and easily on request.

We will not publish any personal information, including photos, on our website without the permission of the relevant individual.

When uploading information to our websites, staff will be considerate of any metadata or deletions which could be accessed in documents and images on the site.

19. CCTV and Photography

We understand that recording images of identifiable individuals constitutes as processing personal information and so it is done in line with data protection principles. Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil a legitimate purpose such as for safety and security. Staff, students and visitors are notified of the purpose for collecting CCTV images via notice boards, letters and email.

All CCTV footage will be kept for six months for security purposes; the Data Protection Officer is responsible for keeping the records secure and allowing access.

We will always indicate our intentions for taking photographs or film of students or at Trust or academy events and will ensure we have permission before publishing them.

20. Data retention

Data will not be kept for longer than is necessary and will be deleted as soon as practicable.

Some educational records relating to former students may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

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

21. Subject access requests

Under the Data Protection Act 1998 and the General Data Protection Regulation 2018 individuals have the right to request access to information any organisation holds about them. This is known as a Subject Access Request (SAR).

A SAR must be made in writing (which can be via email). Before any information is supplied we will need to verify your identity. Children over the age of 12 will need to make a Subject Access Request themselves or given written permission for their parents to be supplied with the information. This is different from a request to see the Education Record – see section xx

A copy of the information will be supplied to the individual free of charge; however, we 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.

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

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, we retain 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 Information Commissioner.

We will not reveal the following information in response to subject access requests:

- Information that might cause serious harm to the physical or mental health of the individual or another individual
- Information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests
- Information contained in adoption and parental order records
- Certain information given to a court in proceedings concerning the child

22. Parental requests to see the educational record

Parents have the right of access to their child's educational record, free of charge, within 15 school days of a request.

Personal data about a child belongs to that child, and not the child's parents. This is the case even where a child is too young to understand the implications of subject access rights.

For a parent to make a subject access request, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

23. Disposal of records

We recognise that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.

All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services.

All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process.

Disposal of IT assets holding data shall be in compliance with ICO guidance: https://ico.org.uk/media/for-organisations/documents/1570/it_asset_disposal_for_organisations.pdf

We will always choose a qualified source for disposal of IT assets and collections.

24. Complaints

Complaints will be dealt with in accordance with Aldridge Education Complaints Procedure. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

26. Contacts

If you have any enquires in relation to this Policy, please contact Liz Dawson, Director of Governance and HR, who will also act as the contact point for any subject access requests. elizabeth.dawson@aldridgeeducation.org

For information about Darwen Aldridge Community Acacdemy, including subject access requests, you should contact Will Ames on 01254 819500 or will.ames@daca.uk.com

Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk or telephone 0303 123 1113.

Appendix A

Student Privacy Notice

We hold personal data about students to support teaching and learning, to provide pastoral care and to assess how the academy is performing. We may also receive data about students from other organisations including, but not limited to, other schools, local authorities and the Department for Education.

The categories of student information that we collect, hold and share include:

- Personal information (such as name, unique pupil number and address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Relevant medical information
- Behavioural information / Exclusions
- Academic progress and Assessment Information
- Special Educational Needs Information
- Use of the IT School Services (to ensure their safe and appropriate use)
- Biometric information (cashless catering)
- CCTV footage.

Why we collect and use this information

We use the student data:

- to support student learning
- to monitor and report on student progress
- to provide appropriate pastoral care
- to assess the quality of our services
- to be able to administer academy IT services
- to comply with the law regarding data sharing
- to safeguard our students

The lawful basis on which we use this information

We collect and use student information under Article 6, and Article 9 where data processed is special category data from the GDPR-from 25 May 2018 and for data collection purposes under the Education Act 1996 https://www.gov.uk/education/data-collection-and-censuses-for-schools

* What are the lawful bases for processing?

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

The academy has drafted a number of policies to ensure all staff, trustees and governors are aware of their responsibilities and outlines how the academy complies with the following core principles of the GDPR.

Collecting student information

Whilst the majority of student information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain student information to us or if you have a choice in this.

Storing student data

Where information forms part of a student's statutory education record (The Education Regulations 2005 SI 2005 No. 1437), the academy will retain the information for 25 years from the child's date of birth. Other information will be retained only where it is required to perform our legal obligations or where it is retained to safeguard and promote the welfare of children.

http://www.legislation.gov.uk/uksi/2005/1437/made

Who we share student information with

We routinely share student information with:

- schools that the student attends after leaving us
- our local authority
- Aldridge Education
- the Department for Education (DfE)
- the NHS

Why we share student information

We do not share information about our student with anyone without consent unless the law and our policies allow us to do so.

We share students' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our student with the (DfE) under regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

Data collection requirements:

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

Youth support services

Students aged 13+

Once our students reach the age of 13, we also pass student information to our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- youth support services
- careers advisers

A parent or guardian can request that **only** their child's name, address and date of birth is passed to their local authority or provider of youth support services by informing us. This right is transferred to the child / student once they reach the age 16.

Students aged 16+

We will also share certain information about students aged 16+ with our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- post-16 education and training providers
- youth support services
- careers advisers

For more information about services for young people, please visit our local authority website.

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about students in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical

purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our students to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The Department for Education may share information about our students from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department for Education has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether Department for Education releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to student information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the Department for Education has provided student information, (and for which project), please visit the following website: https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

Requesting access to your personal data

Under data protection legislation, parents and students have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact: Will Ames on 01254 819500 or will.ames@daca.uk.com

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and

- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, please contact Will Ames on 01254 819500 or will.ames@daca.uk.com. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact

If you would like to discuss anything in this privacy notice, please contact Will Ames on 01254 819500 or will.ames@daca.uk.com for further information.

May 2018

Staff Privacy Notice

We process data relating to those we employ to work at, or otherwise engage to work at, within Aldridge Education (the Trust). The purpose of processing this data is to assist in the running of the Trust and its academies.

The categories of school workforce information that we collect, process, hold and share includes:

- personal information (such as name, employee or teacher number, national insurance number, contact details, DBS, bank account)
- special categories of data including characteristics information such as gender, age, ethnic group
- contract information (such as start dates, hours worked, post, roles and salary information)
- work absence information (such as number of absences and reasons. details of periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave)
- qualifications (and, where relevant, subjects taught)
- relevant medical information
- assessments of staff performance, including appraisals, performance reviews and ratings, performance improvement plans and related correspondence;
- information about your marital status, next of kin, dependants and emergency contacts
- Use of the IT Academy Services (to ensure their safe and appropriate use)
- Biometric information (such as fingerprints)
- CCTV footage and photographs.

Why we collect and use this information

We use school workforce data to:

- to fulfil our statutory obligations as an employer
- safeguard our students
- improve the quality of teaching and learning
- enable the development of a comprehensive picture of the workforce and how it is deployed
- inform the development of recruitment and retention policies
- comply with the law regarding data sharing
- to facilitate management of Academy IT services

The lawful basis on which we process this information

We collect and use pupil information under Article 6, and Article 9 where data processed is special category data from the General Data Protection Regulations May 2018 (GDPR) and for data collection purposes under the Education Act 1996 https://www.gov.uk/education/data-collection-and-censuses-for-schools

What are the lawful bases for processing?

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

The Trust has drafted a number of policies to ensure all staff, trustees and governors are aware of their responsibilities and outlines how the Trust complies with the core principles of the GDPR.

Collecting this information

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with data protection legislation, we will inform you whether you are required to provide certain school workforce information to us or if you have a choice in this.

Storing this information

The Trust will hold your personal data for the duration of your employment. The periods for which your data is held after the end of employment are set out by the relevant legislation and our backup retention periods.

Who we share this information with

We routinely share this information with:

- the Department for Education (DfE)
- the local authority

Why we share school workforce information

We do not share information about workforce members with anyone without consent unless the law and our policies allow us to do so.

Local authority
We are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Department for Education (DfE)
We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the

assessment educational attainment.

We are required to share information about our staff with the (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Data collection requirements

The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005.

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

To contact the department: https://www.gov.uk/contact-dfe

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact Will Ames on 01254 819500 or will.ames@daca.uk.com

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing

- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed;
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance by contacting Will Ames on 01254 819500 or will.ames@daca.uk.com or Liz Dawson, Director of Governance & HR elizabeth.dawson@aldridgeeducation.org Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Further information

If you would like to discuss anything in this privacy notice, please contact Will Ames on 01254 819500 or will.ames@daca.uk.com or Liz Dawson, Director of Governance & HR elizabeth.dawson@aldridgeeducation.org

Appendix B

Procedures for responding to subject access requests

Rights of access to information

There are two distinct rights of access to information held by schools about students.

1. Under the Data Protection Act 1998 any individual has the right to make a request to access the personal information held about them.

2. The right of those entitled to have access to curricular and educational records as defined within the Education Pupil Information (Wales) Regulations 2004.

These procedures relate to subject access requests made under the Data Protection Act 1998.

Actioning a subject access request

1. Requests for information must be made in writing to the academy (which includes email) Will Ames on 01254 819500 or will.ames@daca.uk.com or for the Trust to info@aldridgeeducation.org

2. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:

    - passport
    - driving licence
    - utility bills with the current address
    - Birth / Marriage certificate
    - P45/P60
    - Credit Card or Mortgage statement

    This list is not exhaustive.

3. Any individual has the right of access to information held about them. However with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Principal should discuss the request with the student and take their views into account when making a decision. A student competent to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

4. We may make a charge for the provision of information, dependent upon the following:

    - Should the information requested contain the educational record then the amount charged will be depend upon the number of pages provided.

    - Should the information requested be personal information that does not include any information contained within educational records schools can charge up to £10 to provide it.

    - If the information requested is only the educational record viewing will be free, but a charge not exceeding the cost of copying the information can be made by the Principal.

5. The response time for subject access requests, once officially received, is one month (irrespective of school holiday periods). However the timeline will not commence until after receipt of fees or clarification of information sought.

6. The GDPR allows exemptions as to the provision of some information; therefore all information will be reviewed prior to disclosure.

7. Third party information is that which has been provided by another, such as the Police, Local Authority, health care professional or another school. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the statutory timescale.

8. Any information which may cause serious harm to the physical or mental health or emotional condition of the student or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

9. If there are concerns over the disclosure of information then additional advice should be sought.

10. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

11. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

12. Information can be provided at the academy with a member of staff on hand to help and explain matters if requested, or provided at face-to-face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail must be used.

Complaints

Complaints about the above procedures should be made to the Director of Governance and HR who will decide whether it is appropriate for the complaint to be dealt with in accordance with the Trust's Complaints Procedure.

Complaints which are not appropriate to be dealt with through the Trust's complaint procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

Contacts

If you have any queries or concerns regarding this Policy advice can be sought from Liz Dawson, Director of Governance and HR elizabeth.dawson@aldridgeeducation.org

Further advice and information can be obtained from the Information Commissioner's Office, www.ico.gov.uk.

Definitions Table

Term	Definition
'We'	Means Aldridge Education or any of its academies
Personal data	Relates to a living individual who can be identified from the data or other information held/likely to be held by the data controller (even where they are not named e.g. from a reference number), including opinions about the individual or what is intended for them. The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria.
Sensitive personal data	Data such as: • Contact details • Racial or ethnic origin • Political opinions • Religious beliefs, or beliefs of a similar nature • Where a person is a member of a trade union • Physical and mental health • Sexual orientation • Whether a person has committed, or is alleged to have committed, an offence • Criminal convictions The GDPR refers to sensitive personal data as "special categories of personal data" (see Article 9). The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.
Processing	Obtaining, recording, holding information, or carrying out operations on data including: • Organisation, adaptation or alteration of data • Retrieval, consultation or use of data • Disclosure of data by transmission, dissemination or other ways of making available • Alignment, combination, blocking, erasure or destruction of data
Data subject	The person whose personal data is held or processed
Data controller	A person or organisation that determines the purposes for which, and the manner in which, personal data is processed
Data	A person, other than an employee of the data controller, who processes the data on behalf

processor	of the data controller
Inaccurate data	Incorrect or misleading data.
Recipient	Anyone to whom data are disclosed unless disclosure is being made as part of a legal inquiry.
Third party	Any person other than the data subject, the data controller, any data processor or other person authorised to process data .