KNUTSFORD MULTI-ACADEMY TRUST

GDPR AND DATA PROTECTION POLICY

Statement of intent

Knutsford Multi-Academy Trust is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the General Data Protection Regulation (GDPR). We are registered as a data controller with the Information Commissioners Office.

Schools within the Trust may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, other academies or schools and educational bodies, and potentially children's services. This policy covers personal data whoever the personal data belongs to and is applicable to all individual schools within the Trust.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the Trust complies with the core principles of the GDPR.

Data Protection is the responsibility of all staff members within individual schools across the Trust.

Monitoring and evaluation

Monitoring and evaluation of this policy will be ongoing throughout the year and will be the responsibility of the Data Protection Officer in partnership with the leadership teams and school business managers of schools within the Trust.

A central record of data protection activity including freedom of information requests, subject access requests and any breaches or near misses, will be kept and reported to the governing body annually.

Any breaches of data protection regulations will be recorded and reported to the data protection officer in time to comply with the 72 hour reporting window.

Legal framework

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

- The General Data Protection Regulation (GDPR)
- The Data Protection Bill 2018 (TBC)
- 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 Academy 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'
- IRMS Data Retention Guidance

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

- Retention Policy
- Photography and Videos
- E-security Policy
- ICT Acceptable Use Policy
- Freedom of Information Policy and Publication Scheme
- CCTV Policy
- Staff handbook guidance of individual schools within the Trust

Applicable data

Personal data refers to information that relates to an identifiable, living individual, including information such as an online identifier. 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.

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

Principles

In compliance with the requirements outlined in the 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;
- 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 – data that is found to be inaccurate for its purpose will either be rectified or deleted;
- 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 due to statutory and contractual purposes and the Academy follows the IRMS data retention guidelines;
- 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.
- Always subject to some form of human processing.

GDPR Individual Rights

This policy reflects the following individual rights:

- The right to be informed
- The right to erasure
- The right to access
- The right to rectification
- The right to data portability
- The right to restrict processing
- The right to object
- The right to not be the subject of any solely automated data processing

(Full details of these can be found in Appendix 2)

Accountability

All staff are responsible for ensuring that they read this policy, the guidance in the Multi-Academy Trust handbook, and comply with it. Where a member of staff has particular responsibility for data compliance, they should make sure they understand their role. Staff are made aware that knowingly or recklessly disclosing personal data may be a criminal offence and that internal disciplinary procedures may be followed if a member of staff commits a data breach. Comprehensive, clear and transparent privacy notices will be provided to staff, pupils and parents reflecting data subjects' right to be informed. (Appendix 1)

Appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR will be implemented by each individual school within the Trust.

A 'data-flow' map and central records of data-processing activities will be maintained, including those relating to higher risk processing such as the processing of special categories data, safeguarding or that in relation to criminal convictions and offences.

Each individual school will keep an Information Asset Register of data controlled by the Trust and its processing activities will include the following:

- Name and details of the organisation

- Purpose(s) of the processing
- Description of the categories of individual and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third parties, 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 through auditing and secure deletion of historic or unnecessary data from databases and sources such as SIMS;
- Transparency in systems, records and training;
- Allowing individuals to monitor processing;
- Continuously creating and improving security features such as migrating all email communications and sharing of data files through proprietary software;
- Using data protection impact assessments where appropriate;
- A central log of data processing activity will be kept for auditing purposes.

Lawful processing

Individual schools within the Trust will process personal data of staff and pupils for the following purposes:

- Administration of education and training;
- Monitoring, reporting, calculation and publication of both exam results and references;
- Safeguarding and pupil welfare;
- The provision of education and training for the planning and control of the curricula and exams;
- The commissioning validation and production of educational materials;
- The arrangement of work experience placements;
- The preparation of DFES returns;
- Recruitment, contractual obligations and performance management of employees;
- Sub-contracting of third party site services such as catering and parent pay systems.

The legal basis for processing different categories of data will be identified and documented in the information asset register prior to data being processed and individuals will be informed of what data is held by the relevant individual schools in the Trust and for what purpose.

Personal data will mainly be processed under one of the following GDPR conditions:

- 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 Trust or individual school;

- For the performance of a contract with the data subject or to take steps to enter into a contract;
- The consent of the data subject or their parents has been obtained.

The following additional conditions may also be applied in certain situations:

- Protecting the vital interests of a data subject or another person in an emergency.
- 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.

Special category 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 in an emergency situation.
    - 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).

Consent

The Trust ensures that consent mechanisms within its data collection processes meets the standards of the GDPR in that it is:

- A positive, opt-in indication;
- Freely given, specific, informed and an unambiguous indication of the individual's wishes;
- Recorded and securely kept as a back-up, documenting how and when consent was given;
- Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR but acceptable consent obtained under the DPA will not be reobtained;
- Able to be withdrawn by the individual at any time;
- Obtained from the parents / guardians of pupils who are under the age of 16 prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child;

- Obtained directly from pupils who are 16 years of age or older.

Data protection officer (DPO)

A DPO has been appointed in order to:

- Inform and advise the Trust and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor the Trust's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.
- The DPO reports to the senior leadership team and the Executive Principal;
- The DPO will operate independently and will not be dismissed or penalised for performing their task.
- Resources and training are provided to the DPO, enabling them to meet their GDPR obligations and develop experience and knowledge.

Data security

Individual schools within the Trust will ensure that:

- Confidential paper records will not be left unattended, in clear view and will be kept in a locked filing cabinet, drawer or safe, with restricted 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 on school servers or cloud-based services off-site;
- Memory sticks will not be used to hold personal information;
- All electronic devices are password-protected to protect the information on the device;
- Where possible, the Trust encrypts electronic devices to allow the remote blocking or deletion of data in case of theft;
- Staff and governors will not use their own personal laptops or computers for Trust purposes;
- All members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their network password and data protection guidance;
- Emails containing sensitive or confidential information are restricted in Microsoft 365 ;
- When sending confidential information, staff will always check that the recipient is correct before sending;
- Where it is necessary for 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 Trust premises accepts full responsibility for the security of the data.

Before sharing any personal data, all staff members will ensure:

- That it is necessary to share the data;
- They are allowed to share it;
- That adequate security, such as email protection filter, 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 schools within 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 put in place.

The Trust takes its duties under the 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 and will be enforced by the DPO in conjunction with either Systems or School Business managers.

Data retention

Data will not be kept for longer than is necessary and follow IRMS guidelines:

- Pupil and Staff Data: 7 years
- Financial Data: 6 years or as laid down by the Academies Financial Handbook
- SEN, Safeguarding, LAC and serious accidents or incidents: 25 years

Unrequired data will be deleted as soon as practicable.

Some educational records relating to former pupils or employees of the Academy 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 under confidential waste procedures, and electronic memories cleansed or destroyed, once the data should no longer be retained.

A record of confidential waste will be kept and managed by the School Business Managers.

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing, consent has been withdrawn or there are legal implications.

Full details are in the **Data Retention Policy**.

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 Trust has ensured that all staff members have been 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 ICO will be informed within 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 by the DPO in consultation with the leadership team.
- 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
- The name and contact details of the DPO
- 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.

Data Protection Impact Assessments

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

DPIAs 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.

DPIAs will be recorded within the Trust's central record of data processing activity and/or the information asset register.

A DPIA will be carried out by the Trust's DPO and appropriate staff 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 data processing activity or project, where necessary.

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

- Safeguarding;
- 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;
- Requests for information from organisations such as the police, NHS or Social Services;
- Issues pertaining to DBS.

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 GDPR.

Publication of information

In accordance with the Freedom of Information Act 2000, Knutsford Multi-Academy 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.

Knutsford Multi-Academy Trust will not publish any personal information, including photos, on its website without the permission of the affected individual.

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

Publication of information onto the website is controlled by the Academy's Marketing manager.

Disclosure of Data through Subject Access Requests or Freedom of Information

The GDPR right of access grants individuals the right to seek confirmation of and access to any data which is processed about them by Knutsford Multi Academy Trust.

Personal data will only be disclosed to third parties in two circumstances:

- Where the data subject has given consent (or in the case of a child without capacity under the Data Protection Act - ordinarily those under 12 years of age - their parent or guardian);
- Where the Trust is required or permitted by law to disclose it.

Knutsford Multi Academy Trust will take reasonable steps to confirm the identity of a third party requesting personal data through either a Subject Access Request (SAR) or Freedom of Information (FOI) request and will provide advice and assistance as necessary to the requester.

A **Subject Access Request** allows an individual:

- To verify that their data is being processed
- To access to their personal data and other supplementary data which corresponds to the information provided in the Trust's privacy notices.

Where a person wishes to make a Subject Access Request, they must make a request in writing to the Trust's Data Protection Officer who will check the identity of the requester and respond in an appropriate and secure manner, ideally in person, within one month of receipt. The DPO will clarify the exact nature and scope of the request if needed and work with the appropriate staff to collate the information.

No charge will be made for a SAR unless it is deemed excessive, unfounded or repetitive in nature. The request may be refused in whole or in part if the Trust has legal grounds not to comply with the request in full. Where a request is turned down full reasons for the refusal will be given.

In the event of numerous or complex requests, the period of compliance will be extended by a further two months. An extension may also be necessary if a request is received during the summer holiday. The individual requester 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.

Freedom of Information requests will also be made and dealt with in the same manner as for a SAR. They will be responded to appropriately within the limit of 20 working days. No specific data will be collected in response to an FOI enquiry and the requester will be informed clearly whether or not the Trust holds the requested information.

All SAR and FOI requests and outcomes will be centrally logged.

CCTV

The Trust understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with GDPR principles.

The Trust notifies all pupils, staff and visitors of the purpose for collecting CCTV images via its privacy notices and signage.

Cameras are only placed where they do not intrude on anyone's privacy and are used to:

- Secure the safety of pupils and employees;
- Assist in the management of the school;
- Protect the school building and its assets from criminal damage;
- Identify and prosecute offenders.

All CCTV footage will be kept for 10 days for the purposes described above before being recorded over. The School Business Manager is responsible for keeping the records secure and facilitating access in consultation with the Data Protection Officer.

Full details are in the CCTV policy.

Photography and Videos

The Trust will always indicate its intentions for taking photographs of pupils and will retrieve consent before publishing them.

If the Trust wishes to use images/video footage of pupils in a publication, such as the Trust website, prospectus, or recordings of Trust plays, written consent will be sought for the particular usage from the parent of the pupil if under 16 years of age or the individual pupil if 16 or older.

Precautions, as outlined in the Photography and Videos Policy are taken when publishing photographs of pupils, in print, video or on the Trust website.

Images captured at school events by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR but schools within the Trust will ask parents and family not to post such images online.

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 be duplicated.

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

Recruitment

Knutsford Multi-Academy Trust will collect information from candidates applying for a position. The application form will ask for information relevant to the position applied for and the applicant's explicit consent, both for the data revealed by them and for any request which will be submitted to a third party for personal data about the applicant. The applicant will be informed of:

- Why the school/academy collects the information;
- How long it will be kept;
- The security in place to protect the information;
- How the application will be processed;
- How the information given will be verified;
- They will also be informed of their right to access the data and correct any inaccuracies.

All application information will be securely destroyed under confidential waste procedure unless it is needed.

Policy review

This policy is reviewed every year by the Data Protection Officer and the Headteacher.

The next scheduled review date for this policy is May 2019.

Policy lead:	**Christopher Parr**
Last review date:	**May 2018**
Next review date:	**May 2019**
Approval needed by:	**Headteacher**

Appendix 1

KNUTSFORD MULTI ACADEMY TRUST
DATA PRIVACY NOTICE FOR PUPILS, PARENTS, CARERS AND GUARDIANS
Data Protection Act 1998, General Data Protection Regulation 2018 and Education Act 1996

Categories of Pupil Personal Information

Knutsford Multi-Academy Trust is a 'data controller' which collects and processes pupil information such as:

- Personal identification (such as pupil and parent names, contact details and address, unique pupil number, ID photographs for the school database);
- Characteristics (such as ethnicity*, language and free school meal eligibility);
- Attendance (such as sessions attended, number of absences and absence reasons);
- Behaviour (such as rewards, demerits, exclusions and alternative provision);
- Assessment and attainment (such as internal and external test results, course enrolment;
- Special educational needs (such as the need and ranking);
- Safeguarding (such as court orders and professional involvement)
- Medical and administrative* (such as doctor's information, allergies, medication and dietary requirements);
- Extra-curricular (such as trips, activities and external success);
- Unique learner number (ULN) for post-14 qualifications;
- Post-16 learning information.

(* is 'Special Category' information)

Reasons for Using Pupil Information

We hold and use this personal information to carry out our tasks as a school in the public interest and exercising our official authority. These include:

- To support pupil learning;
- To monitor and report on pupil attainment progress;
- To provide appropriate pastoral care;
- To assess the quality of our services;
- To keep pupils safe;
- To comply with the statutory duties placed upon us for DFE data collection.

Special category information will only be used in the vital or legitimate interests of a pupil. Any decision made about an individual pupil as a result of data processing such as progress analysis or behaviour monitoring will always involve a member of staff.

Collecting Pupil Information

The Trust may receive pupil information from a previous school, the local authority, the Department for Education or the Learning Records Service as well as directly from parents or carers on our admissions form which will make it clear to parents/carers or Year 12 pupils which information must be provided to us and which information is voluntary. We check the accuracy of data each year.
(Visit https://www.gov.uk/education/data-collection-and-censuses-for-schools for more information about the data collection requirements placed on schools by the DFE)

Information Retention

We hold pupil data in line with national IRMS guidelines. This means that we have to retain most pupils' data for a period of 7 years from when they leave. We are required by law to keep SEN, Safeguarding and serious incident data for 25 years from when a pupil leaves.

Information Storage
Each member of staff has received data protection training and will ensure that pupil data will be securely stored within:

- the School's Information Management System (SIMS);
- Microsoft Office 365;
- lockable filing cabinets or drawers.

Sharing of Pupil Information
We do not share information about our pupils with anyone without consent or unless the law allows us to do so. We routinely share pupil data securely with:

- the Department for Education (DfE) on a statutory basis which underpins school funding, educational attainment policy and monitoring within the National Pupil Database as part of the annual census return;
  (Visit https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information or https://www.gov.uk/government/publications/national-pupil-database-requests-received for more information about how the DFE may use and share pupil data)
- schools that the pupils attend after leaving us;
- our local authority;
- examination boards;
- approved educational services including SIMS Capita (Information Management System), SISRA (Progress & Assessment Analysis), Groupcall, Chartwells Caterers, UCAS, Employ (Work Experience Provider), GCSE Pod, Doddle, Mathswatch, Method Maths, Pearson Active Learn.

We may, in the legitimate or vital interests of a pupil, need to also share information with organisations such as the NHS, school nurse, safeguarding agencies or the police. We will not routinely transfer pupil data abroad. Data within Microsoft Office 365 is located within the European Union.

We also share pupil data once they are 13 and/or 16 with our local authority and/or provider of youth support services as they have legal responsibilities for the education or training of 13-19 year olds under the Education Act 1996. This enables them to provide youth support service, careers guidance and post-16 education and training. A parent or guardian can request that **only** their child's name, address and date of birth is shared in this way by informing us. This right is transferred to the pupil once they are 16.

(For more information about services for young people, please visit the local authority website at http://www.cheshireeast.gov.uk/livewell/care-and-support-for-children/services-from-childrens-social-care/youth-offending-and-preventative-services/youth_support.aspx)

Accessing Pupil Data
Individuals have the right under the Data Protection Act 1998 (General Data Protection Regulation) to request a copy of your information and to know what it is used for and how it has been shared. This is called the right of subject access. To make a request or if you have a concern about this privacy notice and how we are collecting or using pupil data, please contact the Trust's Data Protection Officer at **dpo@knutsfordacademy.org.uk**. A copy of our GDPR policy can be found on the Trust website.

Other individual rights can be found in our GDPR policy on the Trust website or at **https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/**

KNUTSFORD MULTI-ACADEMY TRUST
DATA PRIVACY NOTICE FOR STAFF, TRAINEES AND VOLUNTEERS
Data Protection Act 1998, General Data Protection Regulation 2018 and Education Act 1996

Reasons for Using Individuals' Data
Knutsford Multi-Academy Trust is a data controller which collects and processes personal data relating to those we employ to work at, or otherwise engage to work at, our school. This is for employment purposes to assist in the running of the school and/or to enable individuals to be paid.

We hold and use this personal data to:

- improve the management of workforce data across the sector;
- enable development of a comprehensive picture of the workforce and how it is deployed;
- inform the development of recruitment and retention policies;
- allow better financial modelling and planning;
- enable ethnicity and disability monitoring;
- support the work of the School Teachers' Review Body.

Any decision made about an individual as a result of data processing such as analysing appraisal information will always involve a member of staff.

Categories of Data:

- Personal information (such as name, NI number);
- Characteristics (such as ethnicity, nationality, country of birth);
- Qualifications;
- Work related information (including employment contracts, remuneration details and absence information);
- Relevant medical information.

Collecting data
The Trust will receive data from the individual directly and also from previous employers, educational establishments, Disclosure and Barring Service, Department of Education, teacher training organisations and occupational health providers. 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.

Data Retention
We hold workforce data in line with national IRMS guidelines. At present, this is for 7 years after a staff member has left the organisation. We are required by law to keep records relating to accident or injury at work for 12 years from the date of the incident.

Data Storage
Appropriate staff have received data protection training and will ensure that individual data will be securely stored within:

- the School's Information Management System (SIMS);
- Microsoft 365 cloud services
- lockable filing cabinets, cupboards or drawers

Sharing of Individual Data
We will not share information about you with anyone without your consent unless the law allows us to.

We routinely share individuals' data securely with:

- our local authority;
- the Department for Education (DfE) on a statutory basis as part of the school workforce census return. 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 DfE: https://www.gov.uk/contact-dfe
- former and subsequent employers in the form of employment references;
- our payroll providers;
- our pension providers (Cheshire Pension Fund and Teachers' Pension Fund as appropriate);
- HMRC;
- Cheshire East Human Resources team;
- Occupational Health provider;
- ParentPay;
- Chartwells caterers;
- Examination boards;
- NQT assessment board.

We may, in extreme circumstances, need to also share information with organisations such as:

- the NHS;
- safeguarding agencies;
- the police

Will staff data be transferred abroad and why?
We will not routinely transfer staff data abroad. Data within Microsoft Office 365 is located within the European Union.

Accessing your data
Individuals have the right under the Data Protection Act 1998 (General Data Protection Regulation) to request a copy of your information and to know what it is used for and how it has been shared. This is called the right of subject access.
To make a request or if you have a concern about this privacy notice and how we are collecting or using your data, please contact the Trust's Data Protection Officer at dpo@knutsfordacademy.org.uk

Other individual rights can be found in our GDPR policy on the Trust website or at:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

APPENDIX 2: GDPR INDIVIDUAL RIGHTS

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 child, The Trust will ensure that the privacy notice is written in a clear, plain manner that the child 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 identity and contact details of the controller (and where applicable, the controller's representative) and the DPO.
- 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.

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.

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.

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.

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 child

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 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 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 of the personal data in question.

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 an 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 processing of 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.

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 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.

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 the 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.

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 for 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, where 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 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.

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 risk to the interests and rights of the individual and prevents discriminatory effects.

Automated decisions must not concern a child 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.