KNUTSFORD ACADEMY
DATA PROTECTION POLICY

Policy Lead	**Christopher Parr**
Last review date	**July 2022**
Next review date	**July 2023**
Approval needed by:	**Headteacher**

Statement of intent

Knutsford Academy 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.

Knutsford Academy 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.

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

Data Protection is the responsibility of all staff members at the Academy.

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 at the Academy.

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 if necessary.

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 Academy

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 staff handbook, and comply with it. Where a member of staff has a 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 Academy.

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.

The Academy will keep an Information Asset Register of the data which it controls 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 Academy 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 Academy 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 Academy 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 Academy 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 crossborder 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 Academy ensures that consent mechanisms within its data collection processes meets the standards of the GDPR in that consent 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 Academy and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor the Academy'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

The Academy 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 Academy 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 Academy 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 Academy containing sensitive information are supervised at all times.
- The physical security of The Academy'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 Academy 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 Files: current year + 6 years / 25 years from date of birth
- SEN, Safeguarding and serious accidents or incidents: 25 years from date of birth and then review
- Staff Data: Termination of employment + 6 years
- Child protection allegations against staff: Until retirement or 10 years from the date of the allegation
- Financial Data: 6 years or as laid down by the Academies Financial Handbook

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 retention schedule details can be found in the **Data Retention Policy** on the website.

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 Academy 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 Academy 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 Academy 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 Academy, 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 Academy as needed to identify the most effective method of complying with The Academy's data protection obligations and meeting individuals' expectations of privacy.

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

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

A DPIA will be carried out by The Academy'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 Academy 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 Academy 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 Academy 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 Academy will not publish any personal information, including photos, on its website without the permission of the affected individual.

When uploading information to The Academy 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 Academy.

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 Academy is required or permitted by law to disclose it.

Knutsford Academy 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 Academy's privacy notices.

Where a person wishes to make a Subject Access Request, they must make a request in writing to The Academy'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 calendar month from the date of the SAR receipt. If this falls on a bank holiday, then the response will be made by the day immediately after. 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 Academy 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 Academy holds the requested information.

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

CCTV

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

The Academy 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.

CCTV footage will be kept for no more than 14 days for the purposes described above before being recorded over. Any footage which is extracted from the system will be stored and shared with the necessary third party if it is appropriate to do so. 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 Academy will always indicate its intentions for taking photographs of pupils and will retrieve consent before publishing them.

If The Academy wishes to use images/video footage of pupils in a publication, such as The Academy 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 Academy 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 Academy 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 Academy 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.

APPENDIX 1: PRIVACY NOTICES

KNUTSFORD ACADEMY DATA PRIVACY NOTICE for Pupils & their Parents / Carers General Data Protection Regulation (GDPR) / Data Protection Act 2018

Last updated 25th October 2019 – please check this information from time to time.

We, Knutsford Academy, are a data controller for the purposes of the Data Protection Act. We collect personal information from pupils and their parents/ carers and may receive information about pupils from their previous school, local authority and/or the Department for Education (DfE).

The categories of pupil information that we collect, hold and share about pupils and parents include:

- Personal information (such as name, unique pupil number, unique learner number and address, school system ID photographs and telephone number)
- 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)
- Special Educational Needs information (such as EHCP reviews, information from specialist assessors and clinical specialists etc.)
- Other personal information including relevant medical information, provided by pupils' parents/ carers, or others who support the wellbeing and education of pupils, which it is necessary to share with the staff looking after a child to ensure their wellbeing and effective education
- Behaviour and achievement information (such as records of incidents, records of achievement awards logged by teachers)
- Assessment information (including the results of external and school assessments)
- Records of tasks set for pupils and feedback given
- Any qualifications held (for older pupils)
- Information about course choices, career aspirations post-16

We use this pupil and parent information to:

- Support pupil learning
- Monitor and report on pupil attainment, progress and attendance
- Keep children safe regarding medical conditions or emergency contacts
- Provide appropriate pastoral care
- Assess the quality of our services
- Comply with the law regarding DFE data collections and data sharing

Any decision made about an individual pupil as a result of using this personal information will always involve a member of staff and never be solely automated.
Under GDPR, the lawful bases which we rely on for processing pupil information are:

We use the data only in ways that are necessary for the education of your child and the normal functioning of the school, and we design our systems to prevent unauthorised access and to manage access appropriately within the organisation.

In some cases, we collect and use pupil information because we need to do so to protect the vital interests of pupils or staff (e.g. with the medical information we process).

Collecting pupil and parent information

The Academy will collect pupil information from previous schools, from the Local Authority (Cheshire East Council), from the Department for Education or from parents and carers during the admissions process. Much of this is mandatory but we will indicate on our data collection and data checking forms whether you are required to provide certain pupil information to us or if you have a choice in this.

Consent

There are some types of information that we use that are not essential for the job we do. We need consent to process:

- Biometric information (the thumb recognition system we use in the canteen)
- Photographs or videos or other information that we take to use for marketing or publicity

(e.g. the school website, Academy Updates or newspaper articles)

In these cases, we ask parents of pupils in Years 7-11, for permission to use the information via the admissions form or, in some cases, an educational visit letter. In the case of Year 12 and 13 pupils, we will seek permission from the individuals themselves during the admissions process.

If pupils do not want us to use information, a photograph or video for publicity or similar they should tell the member of staff at the time or Mr Parr the data protection officer and we will not do so.

Storing pupil and parent information

We hold pupil information for the set amount of time shown in our data retention schedule, which is available on the Academy website, and in line with IRMS guidelines. We expect to retain most pupil information until an individual is 25 years of age. Data is normally archived or deleted securely unless we have received a specific request to delete data from an individual.

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

- the Academy's information management system (SIMS)

- Microsoft Office 365
- lockable cabinets and offices

Cloud services

In common with most schools, we use 'cloud based' services for the storage and processing of some of the data we hold about you. In all cases we remain the data controller and we ensure the services we use are compliant with legislative requirements. We also check that the information is stored only within the EU and do not routinely transfer it abroad. These services include Alps Connect, Capita SIMS, Chartwells caterers, Employ (work experience), Doddle (Science e-learning), EvolveAdvice, FFT
Aspire, Groupcall, Mathswatch, Method Maths, Microsoft Office 365, ParentPay, Pearson Activelearn, SISRA Analytics (progress and assessment analysis), UCAS. In all cases we hold a signed contract with the service provider which requires them to protect pupil information properly and only process it for the purposes we intend.

Who we share pupil information with

We do not share information about our pupils with anyone unless it is a legal requirement or we have appropriate consent from parents/carers or the individual.

We routinely share pupil information with:

- Schools, colleges or similar that pupils attend after leaving us
- Our Local Authority (Cheshire East Council)*
- The Department for Education (DfE)
- The primary school that you attended, to support our collaboration on school improvement.

We may, in extreme circumstances, need to also share information with organisations such as the NHS, school nurse, safeguarding agencies or the police.

* We are required under section 507B of the Education Act 1996 to pass some information about you to our Local Authority (LA) Youth Support Service for young people aged 13-19 years (25 years for pupils with a learning difficulty). We must provide the names and addresses of you and your parent(s), and any further information relevant to the support services' role. We may also share data with post16 providers to secure appropriate support on entry to post-16 education and training. Parents, or pupils if aged 16 or over, can however ask that no information beyond names, addresses and your date of birth be passed to the support service. Please tell Student Services or the Systems Manager (contact details below) if you wish to opt out of this arrangement or if you want to receive a copy of the information that we hold about you.

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils 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 pupils 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.

The Department may share information about our pupils 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 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 DfE 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 pupil 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.

Individual rights to access personal information

Individuals have the right to access their data or educational record, to ask us to correct it where it is wrong and in certain circumstances ask us to delete the data or limit what we do with it. If you want to see what data we hold about you, you can make a subject access request by contacting the Data Protection Officer, or any other member of staff and explaining that you wish to see the data that the school holds about you. We will then provide you with access to what information we hold about you in printed or electronic copies of the data where the law requires us to do this.

If you think that we are not processing your data fairly, correctly and legally then you have the right to complain. The following options are available to you:

1. Contact the Data Protection Officer (details below) to discuss your concerns; most worries should be dealt with successfully by doing this

2. If you are still not happy the Academy has a complaints policy which is published on our website.
3. You may also contact the Information Commissioner's Office which oversees the way we process data. https://ico.org.uk/concerns/

Useful contacts

Christopher Parr, Assistant Headteacher and Data Protection Officer, Knutsford Academy Bexton Road Knutsford Cheshire WA16 0EA Tel: 01565632738 Email dpo@knutsfordacademy.org.uk
The Data Protection Officer, Cheshire East Council 1st Floor Westfields C/O Municipal Buildings Earle Street Crewe CW1 2BJ Tel: 0300 123 5500 Email dp@cheshireeast.gov.uk
Cheshire East Youth Support Service The Youth Support Service Hub 33 Great King Street Macclesfield SK11 6PN Tel: 01625 384320 Online www.cheshireeast.gov.uk/children_and_families/youth_support.aspx
Public Communications Unit, Department for Education Sanctuary Buildings Great Smith Street London SW1P 3BT Tel: 0370 000 2288 Online https://www.gov.uk/contact-dfe

Further information

Further information on school policies and data protection can be found in the following link: https://3vywr6huwat37ur611ljfqt8-wpengine.netdna-ssl.com/wp-content/uploads/GDPR-Policy2018.pdf

Data protection in Cheshire East:
http://www.cheshireeast.gov.uk/council_and_democracy/council_information/data_protection/data_prot ection.aspx

The Department for Education's data sharing process and the national pupil database:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data
https://www.gov.uk/guidance/national-pupil-database-apply-for-a-data-extract
https://www.gov.uk/government/publications/national-pupil-database-requests-received

Guidance on how schools should protect your data:
https://ico.org.uk/your-data-matters/schools/
https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act

KNUTSFORD ACADEMY
DATA PRIVACY NOTICE for Pupils in pupil friendly language **General Data Protection Regulation / Data Protection Act 2018**

The Academy collects personal information about you and use it so that we can do our job as a school. This privacy notice explains to you what information we keep about you as a school, what we do with that information and what your rights are.

The personal information that we collect includes:

- Personal information (such as name, address and telephone number)
- Characteristics (such as ethnicity, gender, and nationality)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Special educational needs information
- Other personal information including relevant medical information, provided by your parents/ carers, or others who help to look after you
- Behaviour and achievement information (such as records of incidents, records of achievement awards)

- Assessment information (including the results of external and school assessments)
- Information about your course choices, career aspirations etc.
- Records of tasks we have set for you and feedback given

We use the information:

- To support your learning and our duty to educate you as well as possible;
- To monitor and report on your progress;
- To provide pastoral care and keep you safe (e.g. so we know when you might need special help, or can contact your parents when we need to);
- To help us improve how school works (e.g. by looking to see what sort of things help you to learn well);
- To comply with the law (e.g. to make sure that we have the information the government requires us to have, and to share with the Department for Education the information that we have to share about you).

Any use of your information always involves a member of staff at some point.

The parent/carer information that we hold includes:

- Personal information such as name, address and contact details (phone number / email address etc.)
- Other personal information that you have volunteered to us which helps us to ensure your wellbeing and effective education

We use the parent/ carer information:

- To enable us to contact parents in an emergency or in relation to the education of a child
- To tell the government things that they are legally entitled to know about the school and its pupils such as where our pupils live
- To help us provide an effective education for you

Why we are allowed to have and use this information

We use the data only in ways that you would expect us to, and we only show it to the people in school who need to see it. We design our systems to stop the data from going missing or ending up in the wrong hands. If you ever worry that your data is not being treated correctly, you should ask to speak to the Academy's Data Protection Officer, which is currently Mr Parr.

Where does the personal information come from?

To begin with the data comes from your previous school and the forms that your parents complete when you join school. The schools and your parents must give this information to us so that we can fulfil our duty as a school and so that we can take the right action in the event of an emergency. We also get some data about you, such as test results, from the government.

We create data about you based on your test results, attendance and behaviour record and so on. We also occasionally record comments about you or your work so that staff can take good care of you and be aware of your needs. This is done so that we can do our job as a school.

Consent

There are some types of information that we use that are not essential for the job we do. In these cases, we ask your permission, or your parents' permission to use the information. You, or your parents can withdraw that permission whenever you want.

We need consent to process:

- Biometric information (the thumb recognition we use in the canteen)
- Photographs or videos or other information that we take to use for marketing or publicity (e.g. the school website, the Academy Update or Year Book, newspaper articles)

In all these cases we obtain consent by getting your parents to sign a consent form when you join school in Year 7 and which we then renew at certain points until the end of Year 11. We seek consent directly from pupils once they enter Years 12 and 13. If you do not want us to take or use a photograph or video for publicity or similar, you just have to tell us and we will stop doing it. We are also training staff to understand that they should always explain why they are taking a photograph or video. We won't ask for your consent if we are recording a lesson as this is sometime how we try to improve how school works.

Storing pupil information

We hold pupil data only for as long as we need it, then it is deleted or shredded. The details of this are set out in our Data Retention Policy which is available on the Academy website. We expect to retain most information until you are 25 unless we have received a specific request to delete data from an individual. We will normally delete a year cohort's information at a time.

Cloud services

In common with most schools, we use 'cloud based' services for the storage and processing of some of the data we hold about you. This means that we store the data on the Internet instead of on a hard drive in school or provide education providers like GCSE Pod or Chartwells, the school caterers, with some information like your name. We are still in control of your data and take the right steps to ensure it remains safe and secure.

Who we share pupil information with

We do not share information about you with anyone else unless the law, our data protection policy or appropriate consent allow us to do so.

If you leave school to go to another school or college then we will pass your educational record on to the new school or college. We also share information about your examination results with the primary school that you attended, so that we can work with them to improve our schools.

We also have to supply some information about you to our Local Authority (LA) and the Department for Education (DFE) – this is a legal obligation. The DFE might share information with other people who are for example researching education but this can only happen where the law allows it to do so, and it has a thorough approval process to make sure it gets these decisions right.

Once you are aged 13 or over, we pass on certain information to the Local Authority Youth Support Service. We must provide the names and addresses of you and your parent(s), and any further information relevant to the support services' role.

We may also share data about you with post-16 providers to secure appropriate support on entry to post-16 education and training, if this is an educational option we know you are considering.

Parents, or pupils if aged 13 or over, can however ask that no information beyond names, addresses and your date of birth be passed to the support service.

We may also, in certain circumstances, need to share your information with organisations like the Police or NHS.

Please tell Pupil Services, the Data Protection Office or the Systems Manager if you want us to limit the information we share with these sorts of providers. We don't ask for your consent to do this normally because we think it is part of doing the job you expect us to do for you as a school.

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about all pupils in schools in England, including you. It provides important and useful evidence that is used in research to improve education.

Your rights

You have the right to access your information, to ask us to correct it where it is wrong and in certain circumstances you can ask us to delete the data or limit what we do with it. If you want to see what data we hold about you, you can make a subject access request by contacting the Data Protection officer, or any other member of staff and explaining that you wish to see the data that the school holds about you. We will assess the request and arrange for a member of staff to sit with you and show you what data we hold about you and answer any specific requests for information that you may have. We will also arrange for printed or electronic copies of the data where the law requires us to do this.

If you think that we are not processing your data fairly, correctly and legally then you may complain.

The following options are available to you:

1) Contact the Data Protection officer (details below) to discuss your concerns; most worries should be dealt with successfully by doing this

2) If you are still not happy the school has a complaints policy which is published on our website.

3) You may also contact the Information Commissioner's Office which oversees the way we process data. https://ico.org.uk/concerns/

Useful contacts

Christopher Parr, Data Protection Officer, Knutsford Academy, Bexton Road, Knutsford WA16 0EA Tel: 01565 632738
The Data Protection Officer, Cheshire East Council 1st Floor Westfields C/O Municipal Buildings Earle Street Crewe CW1 2BJ Tel: 0300 123 5500 Email dp@cheshireeast.gov.uk
Cheshire East Youth Support Service The Youth Support Service Hub 33 Great King Street Macclesfield SK11 6PN Tel: 01625 384320 Online www.cheshireeast.gov.uk/children_and_families/youth_support.aspx
Public Communications Unit, Department for Education Sanctuary Buildings Great Smith Street London SW1P 3BT Tel: 0370 000 2288 Online https://www.gov.uk/contact-dfe

Further information

Further information on school policies and data protection can be found in the following link: https://3vywr6huwat37ur611ljfqt8-wpengine.netdna-ssl.com/wp-content/uploads/GDPR-Policy2018.pdf

Data protection in Cheshire East:
http://www.cheshireeast.gov.uk/council_and_democracy/council_information/data_protection/data_prot ection.aspx

The Department for Education's data sharing process and the national pupil database:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data
https://www.gov.uk/guidance/national-pupil-database-apply-for-a-data-extract
https://www.gov.uk/government/publications/national-pupil-database-requests-received

Guidance on how schools should protect your data:
https://ico.org.uk/your-data-matters/schools/
https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act

KNUTSFORD ACADEMY

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 Academy is a data controller which collects and processes personal data relating to employees, applicants, apprentices, former employees and temporary agency workers in the course of its activities in order to manage the employment relationship.

Categories of Data:

- Personal information (such as name, address and contact details, including email address and telephone number, employee number, teacher number, NI number, nationality and entitlement to work in the UK);
- Characteristics (such as gender, age, ethnic group);
- Qualifications, (and, where relevant, subjects taught), skills, experience and employment history, including start and end dates, with previous employers and with KMAT;
- Contract information (such as start date, hours worked, post, roles and salary information, and including entitlement to benefits such as pensions);
- Information about your marital status and emergency contacts;
- Your suitability to undertake specific posts (through a DBS check in respect of a criminal record (you will be made aware of this at the point of application));
- Work absence information (such as number of absences and reasons);
- Relevant medical information, including whether or not you have a disability for which the organisation needs to make reasonable adjustments;
- Details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence;
- Assessments of your performance, including appraisals, performance reviews and ratings, training you have participated in, performance improvement plans and related correspondence.

We hold and use this personal data:

- To enter into an employment contract with you and to meet our obligations under your employment contract;
- To ensure that we are complying with our legal obligations;
- For legitimate interest in processing personal data before, during and after the end of the employment relationship. For example:
    - processing employee data allows the organisation to run recruitment and selection processes, conduct pre-employment checks, including determining your right to work in the UK, carry ourt DBS checks (where necessary), make offers of employment and provide contracts of employment;

- plan its resources including succession planning, budgetary and financial planning, organisational and development planning, workforce management, administration, business reporting and analytics;
- process payroll, compensation and benefits including salary, tax, salary sacrifice, pensions and business travel and expense management;
- Highlight and manage workplace issues or risks;
- Maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights; ○ Operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace and to carry out internal reviews, investigations and audits;
- Operate and keep a record of employee performance and related processes, to plan for career development, provide workforce development and for education and training purposes;
- Operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled;
- Obtain occupational health advice, to ensure that it complies with duties in relation to individuals with work-related injury and illness or disabilities and to meet its obligations under health and safety law. Ensuring that employees are receiving the pay or other benefits to which they are entitled;
- Administer flexible working arrangements;
- Operate and keep a record of all types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce

management, ensuring that the organisation complies with its duties in relation to leave entitlement, and to ensure that employees receive the pay or other benefits to which they are entitled;

- Manage physical access control, authorise administer, monitor and terminate access to or use of facilities, records, property and infrastructure including communications services such as telephones, laptops and email/internet use;
- Ensure effective general HR and business administration, including communicating with you and facilitating communication between you and other people;
- Provide references on request for current or former employees; ○ Respond to and defend against legal claims; and ○ Maintain and promote equality in the workplace.

Please note that these examples are illustrative and non-exhaustive

Collecting data

The Academy 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 workforce 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;
- Other IT systems including payroll provider's system, Occupational Health Provider's system, email system;
- 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;
- Disclosure and Barring Service;
- Student Loans company;
- 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;
- government agencies;
- Health and Safety Executive.

Will this information be used to take automated decisions about me?
Knutsford Academy does not use this information for those purposes.

Will my data be transferred abroad and why?
Knutsford Academy will not transfer data abroad. The LA does not do this. The DfE would only do it if it met strict conditions (see link above).

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 Academy's Data Protection Officer at dpo@knutsfordacademy.org.uk

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

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 Academy 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 Academy 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 Academy 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 Academy 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 Academy 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 Academy 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 Academy will inform them of the rectification where possible.

Where appropriate, The Academy 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 Academy 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 Academy 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 Academy 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 Academy's processing of personal data.

In the event that processing is restricted, The Academy 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 Academy 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 Academy has verified the accuracy of the data
- Where an individual has objected to the processing and The Academy 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 Academy 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 Academy 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 Academy 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 Academy will provide the information free of charge.

Where feasible, data will be transmitted directly to another organisation at the request of the individual.

The Academy 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 Academy will consider whether providing the information would prejudice the rights of any other individual.

The Academy 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 Academy 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 Academy 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 Academy will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where The Academy 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 Academy will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The Academy 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.

Where the processing activity is outlined above, but is carried out online, The Academy 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 Academy 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 Academy 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 Academy 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.