Caroline Chisholm School

Ambition Confidence Success

Everyone Every Lesson Every Opportunity

GDPR and Data Protection Policy

Author:	
Status:	[Status]
Approval:	Trust board
Date approved:	02/06/2021
Review date:	02/06/2022
Review timescale:	Annual
Keywords:	GDPR data
[Comments]	

Contents

1 Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2 Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

In addition, this policy complies with our funding agreement and articles of association.

Caroline Chisholm Education Trust is registered as the Data Controller with the Information Commissioner's Office (ICO); Registration Number: Z284205X

3 Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: Name (including initials) Identification number Location data Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data, which is more sensitive and so needs more protection, including information about an individual's: Racial or ethnic origin Political opinions Religious or philosophical beliefs Trade union membership Genetics Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes Health – physical or mental Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4 The data controller

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5 Roles and responsibilities

This policy applies to *all staff* employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Trustee board

The Trustee board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is:

School Data Protection Officer
Warwickshire Legal Services,
PO Box 9, Shire Hall,
Warwick
CV34 4RL
schoolDPO@warwickshire.gov.uk,

5.3 Principal

The principal acts as the representative of the data controller on a day-to-day basis.

5.4 School data champion

The schools designated data champion is the HR director.

5.5 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
- With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
- If they have any concerns that this policy is not being followed ○ If they are unsure whether or not they have a lawful basis to use personal data in a particular way
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

6 Data protection principles

The GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles.

7 Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can *fulfil a contract* with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can *comply with a legal obligation*
- The data needs to be processed to ensure the *vital interests* of the individual
- e.g., to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task *in the public interest*, and carry out its official functions
- The data needs to be processed for the *legitimate interests* of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear *consent*

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Staff must only process personal data where it is necessary to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised.

8 Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9 Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data

- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with.
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests may be submitting in writing or verbally and can be sent either to the Data Protection Officer, a member of staff or a Trustee. To enable the request to be accurately responded to, the applicant should be encouraged to make the request in writing and to set out:

- Name of individual
- Name of School
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request, they must immediately forward it to the DPO.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children below the age of 13 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Children aged 13 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

10 Responding to subject access requests.

When responding to requests, we:

- May ask the individual to provide 2 forms of identification.
- May contact the individual via phone to confirm the request was made.
- Will respond without delay and within 1 month of receipt of the request.
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary We will not disclose information if it:
- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which considers administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

10.1 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified based on public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used, and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

11 Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

12 Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners with a PIN code at each transaction if they wish.

Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

13 CCTV

We, along with our Facilities Management Company, MITIE, us CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the school Business Manager, Caroline Chisholm School, 01604 669200.

14 Photographs and videos

As part of our 'public task' of running a school, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

15 Data protection by design and default

We will put measures in place to show that we have integrated data protection into all our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge.
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies, and any other data protection matters; we will also keep a record of attendance.
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant.
- Maintaining records of our processing activities, including:
- For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
- For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

16 Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing, or disclosure, and against accidental or unlawful loss, destruction, or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use.
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access.
- Where personal information needs to be taken off site, staff must sign it in and out from the school office.
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops, and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils, or governors who store personal information on their personal devices are expected to follow the same security procedures as for school owned equipment. (see our Information Security Policy)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

17 Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

18 Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium.
- Safeguarding information being made available to an unauthorised person.
- The theft of a school laptop containing non-encrypted personal data about pupils.

19 Training

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

20 Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary, when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed *annually* and shared with the full trust board.

21 Links with other policies

This data protection policy is linked to our:

- Child Protection and Safeguarding Policy
- Information Security Policy
- CCTV Policy

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO.

The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been.
- Made available to unauthorised people.
- The DPO will alert the principal and the chair of trustees.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.

The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g., emotional distress), including through:

- Loss of control over their data
- Discrimination
- Identify theft or fraud.
- Financial loss
- Unauthorised reversal of pseudonymisation (for example, key-coding)
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned.

If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

The DPO will document the decision (either way) in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school's computer system in an area administered by the DPO.

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

- A description of the nature of the personal data breach including, where possible:
- The categories and approximate number of individuals concerned.
- The categories and approximate number of personal data records concerned.
- The name and contact details of the DPO.
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

- The name and contact details of the DPO.
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.

The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks, or credit card companies.

The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts and cause
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- Records of all breaches will be stored on the school's computer system in an area administered by the DPO.
- The DPO and principal will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches.

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it.
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save, or replicate it in any way.
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.

The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

Appendix 2: Parent and Student Privacy Notice

Who are we?

Caroline Chisolm School is the 'data controller'. This means we are responsible for how your personal information is processed and for what purposes.

Caroline Chisolm School is registered as the Data Controller with the Information Commissioner's Office (ICO); Registration Number: Z284205X.

You can contact the Academy Trust as the Data Controller in writing at:

The Wooldale Centre for Learning
Wootton Fields
Northampton
NN4 6TP
England

What is a Privacy Notice?

A Privacy Notice sets out to individuals how we use any personal information that we hold about them. We are required to publish this information by data protection legislation. This Privacy Notice explains how we process (collect, store, use and share) personal information about our pupils and parents.

What is Personal Information?

Personal information relates to a living individual who can be identified from that information. Identification can be by the information alone or in conjunction with any other information in the data controller's possession or likely to come into such possession.

- 'Special category' personal information relates to personal information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

What personal information do we process about pupils and parents?

The pupil and parent information that we collect, hold and share includes:

- Personal information including a pupil's name, date of birth, unique pupil number and home address.
- Characteristics such as ethnicity, language, and free school meal eligibility
- Attendance information such as sessions attended, number of absences and absence reasons.
- Educational information including records of work, assessment results, relevant medical information, details of pupils' special educational needs, exclusions/behavioural information, post-16 learning information.
- Contact information for parents, carers and other relatives, including telephone numbers, home addresses and e-mail addresses.
- Information about a child's home life, where required as part of necessary safeguarding and welfare processes.

Why do we use personal information?

We use pupil data:

- to support pupil learning
- to monitor and report on pupil progress.
- to provide appropriate pastoral care
- to assess the quality of our services
- to comply with the law regarding data sharing
- to safeguard pupils
- to share medical information with health professionals

Collecting pupil information

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

What are the legal reasons for us to process your personal information?

We are required to process personal information in accordance with data protection legislation and only do so when the law allows us to. The lawful reasons we have for processing personal information are as follows:

To comply with the law

- We collect and use general purpose pupil information in order to meet certain legal requirements and legal obligations placed upon the Academy Trust by law. We therefore are required to this process personal information for such purposes even if you have not consented to us doing so.
- Details of the type of processing that we must undertake, the personal data that is processed, the legislation which requires us to do so and who we may share this information with is set out in Table 1.
- If you would like a copy of or further information regarding the statutory authorities that underpin our legal obligations, you should contact the Academy Trust in writing.

To protect someone's vital interests

- We are able to process personal information when there is an emergency and/or where a person's life is in danger.

With the consent of the individual to whom that information 'belongs'

- Whilst much of the personal information processed is in accordance with a legal requirement, there is some personal information that we can only process when we have your consent to do so. In these circumstances, we will provide you with specific and explicit information regarding the reasons the data is being collected and how the data will be used.

To perform a public task

- It is a day-to-day function of the Academy Trust to ensure that children receive the education and support they require. Much of this work is not set out directly in any legislation but it is deemed to be necessary in order to ensure that pupils are properly educated and supported
- Please be aware that an individual has the right to object to any processing where it is likely to cause or is causing harm or distress. To exercise this right, individuals should do so by contacting the academy trust to inform them of their reasons for the objection. These reasons should relate to your specific circumstances. Upon receipt of an objection, the academy trust will consider the reasons for the objection and balance this against the legitimate grounds to process data.

We have a legitimate interest

- Occasionally we have reasons to process information which fall outside of our usual day-to-day school functions. Details of the type of processing that we may undertake on this basis are set out in Table 1.
- Please be aware that an individual has the right to object to any processing where it is likely to cause or is causing harm or distress. To exercise this right, individuals should do so by contacting the academy trust to inform them of their reasons for the objection. These reasons should relate to your specific circumstances. Upon receipt of an objection, the academy trust will consider the reasons for the objection and balance this against the legitimate grounds to process data.

Special category personal information

In order to process 'special category' data, we must be able to demonstrate how the law allows us to do so. In additional to the lawful reasons above, we must also be satisfied that ONE of the following additional lawful reasons applies:

- Explicit consent of the data subject
- Processing relates to personal data which is manifestly made public by the data subject
- Necessary for establishing, exercising, or defending legal claims
- Necessary for reasons of substantial public interest
- Necessary for preventive or occupational medicine, or for reasons of public interest in the area of public health
- Necessary for archiving, historical research or statistical purposes in the public interest

The lawful reasons for each type of special category personal information data that we process is set out in the tables attached.

Who might we share your information with?

We routinely share pupil information with:

- schools that the pupils attend after leaving us
- our local authority
- the Department for Education (DfE)
- Educators and examining bodies.
- Our auditors
- NHS
- Public Health and other public health agencies
- Information Management software and linked systems; SIMS, Groupcall Xporter, Wonde

We do not share information about our pupils or parents unless the law and our policies allow us to do so.

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

This enables them to provide services as follows:

- youth support services
- careers advisers

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

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

This enables them to provide services as follows:

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

We are also required, by law, to pass certain information about pupils to specified external bodies, such as our local authority and the Department for Education, so that they are able to meet their statutory obligations.

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.

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

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.

For more information about the department's data sharing process, please visit:

https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

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

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

Data collection requirements:

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

What do we do with your information?

All personal information is held in a manner which is compliant with data protection legislation. Personal information is only processed for the purpose it was collected The Academy Trust monitors the personal information it processes and will only share personal information with a third party if it has a legal basis to do so (as set out above).

Covid-19 – Data Collection Requirements:

It may be necessary for us to share limited information with the Department of Public Health if an individual tests positive for Coronavirus, or if there is a Coronavirus outbreak. This will enable the named agencies to liaise with families to provide advice and support, and to take appropriate steps in responding to an outbreak.

Testing in schools

To enable lateral flow testing in schools, we need to process personal data of pupils taking part. For information on the data processed in relation to testing in schools, please refer to the privacy information provided by the DfE and published on our website:

https://mcusercontent.com/542114d67cb9753f9f1304a54/files/7327b011-e5e6-452b-9fb0-e4c483fb29b3/Privacy_Notice_for_supply_of_contact_details_by_schools_and_colleges_for_management_of_Covid_19_testing.pdf

How long do we keep your information for?

In retaining personal information, the Academy Trust complies with the Retention Schedules provided by the Information Record Management Society. The schedules set out the Statutory Provisions under which the Academy Trust are required to retain the information.

A copy of those schedules can be located using the following link: http://irms.org.uk/page/SchoolsToolkit

Transferring data internationally

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

What are your rights with respect of your personal information?

Under data protection law, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or to have access to your child's educational record contact the school or the School Data Protection Officer at Warwickshire Legal Services via email at schooldpo@warwickshire.gov.uk or alternatively.

School Data Protection Officer
Warwickshire Legal Services
Warwickshire County Council
Shire Hall
Warwick
CV34 4RL
***Please ensure you specify which school your request relates to.*

Where the academy trust process data for the purposes of legitimate interests or to fulfil their public task, individuals have a right to object to the processing where it is likely to cause, or is causing, harm or distress. When

exercising this right, individuals should contact the academy trust to inform them of their reasons for their objection. The academy trust will consider the reasons for any objection and asses the risk to the individual against the purposes for the processing. In the event the academy trust is unable to comply with an objection, we will ensure we can demonstrate compelling legitimate grounds to continue with the processing.

You also have the right to:

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

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/

Review

The content of this Privacy Notice will be reviewed every 12 months.

Table 1 - Personal information we are required to process to comply with the law.

Information Type	Relevant legislation	Special Category– additional lawful reason	Third Parties with whom we share the information	Lawful reason for sharing
Special Education Needs Report	Children's and Families Act 2014, section 69		Local Authority	Legal Obligation
Attendance register	Education (Pupil Registration) (England) Regulations 2006, Regulation 4, 10, 11 and 12		OFSTED, Local Authority	Legal Obligation
Common Transfer file	Education (Pupil Registration) (England) Regulations 2005, Regulation 6		School pupil transfers to	Legal Obligation
Safeguarding information	Education Act 2002, section 175 Children's Act 1989, Section 17, 47, 83. Children's Act 2004, Section 11		Local Authority	Legal Obligation
Admissions Register	Education (Pupil Registration) (England) Regulations 2006, Regulation 4, 10, 11, 14 and 15		OFSTED, Local Authority	Legal Obligation
Curricular Record including Assessment and achievement data	Education (Pupil Information) (England) Regulations 2005, Regulation 4		OFSTED, Local School. Local Authority	Legal Obligation
Educational Record	Education (Pupil Information) (England) Regulations 2005, Regulation 5 and 6		Parents, Local school	Legal Obligation
Pupil Information i.e name, age address, Emergency contact details	Education (Information About Individual Pupils) (England) Regulations 2013, Regulation 3 and 5		Department of Education – school census. Other schools – when pupils transfers	Legal Obligation
Medical / Dietary / allergies		Necessary for preventative or occupational medicine	Department of Education – school census. Other schools – when pupils transfers	Legal Obligation
School Census	Education Act 1996, Sections 537 & 537A, and accompanying regulations		Department of Education	Legal Obligation

Information Type	Relevant legislation	Special Category– additional lawful reason	Third Parties with whom we share the information	Lawful reason for sharing
Staff information, including personal details, DBS check, qualifications	Education Act 2005, section 114		Secretary of State, Warwickshire County Council, Disclosure and Barring Service	Legal Obligation

Table 2 - Personal information we are required to process as it is necessary to protect someone's vital interests.

Information Type	Special Category - additional lawful reason	Third Parties with whom we share the information	Lawful reason for sharing
Medical Information	Necessary to protect vital interests of the data subject or another person where the data subject is physically or legally incapable of giving consent'	Medical staff i.e., paramedics/ambulance	Vital Interest
Religious belief	Necessary to protect vital interests of the data subject or another person where the data subject is physically or legally incapable of giving consent'	Medical staff i.e., paramedics/ambulance	Vital Interest

Table 3 - Personal information we are required to process with the consent of the individual to whom that information 'belongs'.

Information Type	Special Category - additional lawful reason	Third Parties with whom we share the information	Lawful reason for sharing
Photographs		Government agencies, e.g., Department for Education,	Consent
Email address		Not shared	

Table 4 - Personal information we are required to process because it is necessary to do so in order to perform a public task.

Information Type	Special Category - additional lawful reason	Third Parties with whom we share the information	Lawful reason for sharing
Pupil Information i.e., name, age address, Parent detail, Emergency contact details		Department of Education – school census. Other schools – when pupils transfers	Legal Obligation
Academic Progress data including Leaving data, welcome data. Learning journals, staff observations		OFSTED, Parents, Health such as Speech and Language	Public Task & Legal Obligation
Safeguarding information, Medical, Special Education Needs		Local Authority, Health, Parents	Legal Obligation
Educational and Safeguarding Information used internally for the purpose of educating and protecting the welfare of children.			

Table 5 - Personal information we process because we have a legitimate interest

Information Type	Special Category - additional lawful reason	Third Parties with whom we share the information	Lawful reason for sharing
Images captured on our CCTV system	n/a	This is not shared routinely	n/a