Cavendish Close
Infant and Nursery School

Contents

CAVENDISH CLOSE INFANT AND NURSERY SCHOOL

Data Protection Policy 2021

Cavendish Close Infant School is committed to working effectively to provide a secure environment to protect data that we hold and store. Whilst there is a statutory duty that is important, the fact that we store data about individuals means that we are responsible for your data and we take that very seriously. This policy, and the Privacy Notices, sets out how we look after and use data.

Each school will be responsible for the day to day management of data that is held about pupils, staff, parents, carers and other individuals in connection with that school.

Where we use the phrase 'we' that refers to the school.

What is the General Data Protection Regulation (UK GDPR)?

This is a European Directive that was brought into UK law with an updated Data Protection Act 2018 (DPA) in May 2018. It was brought into line with changes to the UK leaving the Eu on 31 December 2020.

The UK GDPR and DPA 2018 exist to look after individuals' data. It is a series of safeguards for every individual. Information about individuals needs to be treated with respect and be secure.

The UK GDPR exists to protect individual rights in an increasingly digital world.

Who does it apply to?

Everyone, including schools. As 'Public Bodies' schools and trusts have more obligations than some small businesses. It is mandatory to comply with the UK GDPR and proposed provisions in the Data Protection Act 2018.

We want to make sure information about pupils, parents, staff and volunteers is kept secure and within the law.

What is Data?

Any information that relates to a living person that identifies them. This can be by name, address or phone number for example. It also relates to details about that person, which can include opinions.

Some data is considered to be more sensitive, and therefore more important to protect. This is information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sex life and sexual orientation, genetic data, and biometric data where processed to uniquely identify a person.

Schools often collect sensitive data for DfE and LA requirements and of course pupil data may contain information about safeguarding, SEN or health needs. Information about other family members may also be on the school file.

Privacy Notices that explain how data about specific groups or activities is used and stored are also available. These can be obtained from each school and links on the website to UK GDPR compliance.

What are the key principles of the UK GDPR?

Lawfulness, transparency and fairness

Schools must have a legitimate reason to hold the data, we explain this in the Data Privacy Notices. We often ask for consent to use data about a pupil for a particular purpose. If you wish to withdraw consent we have a form to complete to allow us to process your request. There are some times when you cannot withdraw consent as explained in 'Data Subjects' Rights'.

Collect data for a specific purpose and use it for that purpose

Data cannot be used for a purpose that it was not originally collected for, or where notice has not been given about how data may be used after collection.

Limited collection

Data Controllers should only collect the minimum amount of data needed for a particular task or reason. If there is a breach or a hack only limited information can be lost.

Accuracy

Data collected should be accurate, and steps should be taken to check and confirm accuracy. This is done when pupils join the school and is reviewed on an annual basis.

If a Data Subject feels that the information held is inaccurate, should no longer be held by the Controller or should not be held by the Controller in any event, a dispute resolution process and complaint process can be accessed, using the suitable forms. Initially an approach should be made directly to the individual school.

Retention

A retention policy is in place that governs how long records are held for.

Security

We have processes in place to keep data safe. That might be paper files, electronic records or other information. Please see Information Security Policy.

Who is a 'data subject'?

An individual whose details we keep on file. Some details are more sensitive than others. The UK GDPR sets out collection of details such as health conditions and ethnicity which are more sensitive than names and phone numbers.

Data subjects' rights

Individuals have a right:-

- to be informed
- of access to data stored about them or their children
- to rectification if there is an error on the data stored
- to erasure if there is no longer a need for school to keep the data
- to restrict processing, i.e. to limit what is done with their data
- to object to data being shared or collected

There are other rights that relate to automated decision making and data portability that are not directly relevant in schools.

Data subjects' rights are also subject to child protection and safeguarding concerns and sharing information for the prevention and detection of crime. Schools also have legal and contractual obligations to share information with organisations such as the Department for Education, Social Care, the Local Authority and HMRC amongst others. In some cases these obligations override individual rights.

These Data Subject's Rights are set out in more detail in the document 'My Rights – A Guide for Data Subjects'.

Subject Access Requests

You can ask for copies of information that we hold about you or a pupil (who you have parental responsibility for). This Subject Access Request process is set out separately. You need to fill out the form, and you may need to provide identification evidence for us to process the request.

We have to provide the information within a month, but this can be extended if the request is complicated or the data cannot be accessed.

When we receive a request, we may ask you to be more specific about the information that you require. This is to refine any queries to make sure you access what you need, rather than sometimes getting a lot of information that may not be relevant to your query.

In some cases, we cannot share all information we hold on file if there are contractual, legal or regulatory reasons.

We cannot release information provided by a third party without their consent, or in some cases you may be better to approach them directly, e.g. school nurses who are employed by the NHS.

We will supply the information by paper or electronic form.

If you wish to complain about the process, please see our Complaints Policy and later information in this DPA policy.

Who is a 'Data Controller'?

The academy trust is the Data Controller. They have ultimate responsibility for how the schools manage data. They delegate this processing to individuals to act on their behalf, that is the trust central team and the relevant school staff in each setting.

The data controller can also have contracts and agreements in place with outside agencies who are data processors.

Who is a 'Data Processor'?

This is a person or organisation that uses, collects, accesses or amends the data that the controller has collected or authorised to be collected. It can be a member of staff, a third-party company, possibly a governor, a contractor or temporary employee. It can also be another organisation such as the police or the Local Authority.

Data Controllers must make sure that Data Processors are as careful about the data as the controller themselves. The UK GDPR places additional obligations on organisations to make sure that Data Controllers require contractual agreements to ensure that this is the case.

Processing data

The Trust and the schools must have a reason to process the data about an individual. Our Privacy Notices set out how we use data. The UK GDPR has 6 conditions for lawful processing and any time we process data relating to an individual it is within one of those conditions.

If there is a data breach we have a separate policy and procedure to follow to take immediate action to remedy the situation as quickly as possible.

The legal basis and authority for collecting and processing data in school are:-

- consent obtained from the data subject or their parent
- performance of a contract where the data subject is a party
- compliance with a legal obligation
- to protect the vital interests of the data subject or other associated person
- to carry out the processing that is in the public interest and/or official authority
- it is necessary for the legitimate interests of the data controller or third party
- in accordance with national law.

In addition, any special categories of personal data are processed on the grounds of

- explicit consent from the data subject or about their child
- necessary to comply with employment rights or obligations
- protection of the vital interests of the data subject or associated person
- being necessary to comply with the legitimate activities of the school
- existing personal data that has been made public by the data subject and is no longer confidential
- bringing or defending legal claims
- safeguarding
- national laws in terms of processing genetic, biometric or health data.

Processing data is recorded within the school systems.

Data Sharing

Data sharing is done within the limits set by the UK GDPR. Guidance from the Department for Education, health, the police, local authorities and other specialist organisations may be used to determine whether data is shared.

The basis for sharing or not sharing data is recorded in school.

Breaches & Non Compliance

If there is non compliance with the policy or processes, or there is a DPA breach as described within the UK GDPR and DPA 2018 then the guidance set out in the Breach & Non Compliance Procedure and Process needs to be followed.

Protecting data and maintaining Data Subjects' rights is the purpose of this policy and associated procedures.

Consent

As a trust, where required, we will seek consent from staff, volunteers, young people, parents and carers to collect and process their data. We will be clear about our reasons for requesting the data and how we will use it. There are contractual, statutory and regulatory occasions when consent is not required.

Consent is defined by the UK GDPR as “any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”.

We may seek consent from young people also, and this will be dependent on the child and the reason for processing.

This will largely be managed in individual schools.

Consent and Renewal

On the trust/school websites we have ‘Privacy Notices’ that explain how data is collected and used. It is important to read those notices as it explains how data is used in detail.

Obtaining clear consent, where required, and ensuring that the consent remains in place is important for school. We also want to ensure the accuracy of that information.

For Pupils and Parents/Carers

On joining the school you will be asked to complete a form giving next of kin details, emergency contact and other essential information. We will also ask you to give consent to use the information for other in-school purposes, as set out on the data collection/consent form.

The contact and consent form is reviewed on an annual basis. It is important to inform school if details or your decision about consent changes. A form is available. This is the obligation of each individual to notify the school of changes.

Pupil Consent Procedure

Where processing relates to a child under 13 years old, school will obtain the consent from a person who has parental responsibility for the child as required.

Pupils may be asked to give consent or to be consulted about how their data is obtained, shared and used in certain situations.

Withdrawal of Consent

Consent can be withdrawn, subject to contractual, statutory or regulatory constraints. Where more than one person has the ability to provide or withdraw consent the school will consider each situation on the merits and within the principles of UK GDPR and also child welfare, protection and safeguarding principles.

Please complete the appropriate form.

CCTV Policy

Please also see the CCTV and IT Security policy. We use CCTV and store images for a period of time in line with the policy. CCTV may be used for:-

- Detection and prevention of crime
- School staff disciplinary procedures
- Pupil behaviour and exclusion management processes
- To assist the school in complying with legal and regulatory obligations

Data Protection Officer

We have a Data Protection Officer whose role is:-

- to inform and advise the controller or the processor and the employees who carry out processing of their obligations under the UK GDPR

- to monitor compliance with the UK GDPR and DPA

- to provide advice where requested about the data protection impact assessment and monitor its performance

- To be the point of contact for Data Subjects if there are concerns about data protection

- to cooperate with the supervisory authority and manage the breach procedure

- to advise about training and CPD for the UK GDPR

Our DPO is John Walker whose contact details are:

Address:
Office 7, The Courtyard
Gaulby Lane,
Stoughton
LE2 2FL

Email info@jawalker.co.uk

Physical Security

In school, every secure area has individuals who are responsible for ensuring that the space is securely maintained and controlled if unoccupied, i.e. locked. Offices and cupboards that contain personal data should be secured if the processor is not present.

The Premises Manager/supervisor is responsible for authorising access to secure areas along with SLT/business Manager.

All Staff, contractors and third parties who have control over lockable areas must take due care to prevent data breaches.

All sites and locations need to have the suitable security and review measures in place.

Secure Disposal

When disposal of items is necessary a suitable process must be used. This is to secure the data, to provide a process that does not enable data to be shared in error, by malicious or criminal intent.

These processes, when undertaken by a third party are subject to contractual conditions to ensure UK GDPR and DPA compliance.

Complaints & the Information Commissioner Office (ICO)

The school Complaint Policy deals with complaints about Data Protection issues.

There is a right to complain if you feel that data has been shared without consent or lawful authority.

You can complain if you have asked to us to erase, rectify, or not process data and we have not agreed to your request.

We will always try to resolve issues on an informal basis, and then through our formal complaints procedure. Please complete the form, and we will contact you with more details about the timescale and process.

In the UK it is the ICO who has responsibility for safeguarding and enforcing the DPA

obligations. Email: casework@ico.org.uk Helpline: 0303 123 1113 web: www.ico.org.uk

Review

A review of the effectiveness of UK GDPR compliance and processes will be conducted by the Data Protection Officer every 12/24 months.

Data Protection Breach & Non Compliance Procedure

All staff and governors must be aware of what to do in the event of a DPA / UK GDPR breach. The

'Data Breach Flowchart' outlines the process.

The 'Data Breach Form' must be completed and updated as the process progresses.

Most breaches, aside from cyber criminal attacks, occur as a result of human error. They are not malicious in origin and if quickly reported are often manageable.

Everyone needs to understand that if a breach occurs it must be swiftly reported.

What is a breach?

A personal data breach means a breach of security leading to the destruction, loss, alteration,

unauthorised disclosure of, or access to, personal data. This means that a breach is more than just

losing personal data.

Examples of breaches are:-

- Information being posted to an incorrect address which results in an unintended recipient reading that information
- Loss of mobile or portable data device, unencrypted mobile phone, USB memory stick or similar
- Sending an email with personal data to the wrong person
- Dropping or leaving documents containing personal data in a public place
- Personal data being left unattended at a printer enabling unauthorised persons to read that information
- Not securing documents containing personal data (at home or work) when left unattended
- Anything that enables an unauthorised individual access to school buildings or computer systems
- Discussing personal data with someone not entitled to it, either by phone or in person. How can you be sure they are entitled to that information?
- Deliberately accessing, or attempting to access or use personal data beyond the requirements of an individual's job role e.g. for personal, commercial or political use. This action may constitute a criminal offence under the Computer Misuse Act as well as the Data Protection Act.
- Opening a malicious email attachment or clicking on a link from an external or unfamiliar source, which leads to school's equipment (and subsequently its records) being subjected to a virus or malicious attack, which results in unauthorised access to, loss, destruction or damage to personal data.

What to do?

Being open about the possible breach and explaining what has been lost or potentially accessed is an important element of working with the ICO and to mitigate the impact. Covering up a breach is never acceptable and may be a criminal, civil or disciplinary matter.

Report the breach to the Data Controller, Data Protection Compliance Manager and DPO as soon as possible, this is essential.

What happens next?

The breach notification form will be completed and the breach register updated.

Advice will be sought from the DPO. Consideration is given about how to effectively manage the breach, who to inform and how to proceed.
If the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach notification to those people will be done in a co-ordinated manner with support from the DPO.

Actions and changes to procedures , additional training or other measures may be required to be implemented and reviewed.

The breach report will be within 72 hours of becoming aware of the breach.
It may not be possible to investigate the breach fully within the 72 hour timeframe. Information about further investigations will be shared with the ICO with support from the DPO.

Procedure – Breach notification data controller to data subject

For every breach the school will consider notification to the data subject or subjects as part of the process. If the breach is likely to be high risk they will be notified as soon as possible and kept informed of actions and outcomes.

The breach and process will be described in clear and plain language.

If the breach affects a high volume of data subjects and personal data records, the most effective form of notification will be used and discussed with the Data Controller with support from the Data Protection Compliance Manager and DPO.

Advice will be taken from the ICO about how to manage communication with data subjects if appropriate.

A post breach action plan will be put into place and reviewed.

Evidence Collection

It may be necessary to collect information about how an information security breach or unauthorised release of data occurred. This evidence gathering process may be used as an internal process (which can include disciplinary proceedings), it may be a source of information for the ICO, it could also be used within criminal or civil proceedings.

This process will be conducted by a suitable member of school staff, which may be the Data Management Compliance Officer or Data Protection Officer, but will be determined depending on the nature of the breach.

Guidance may be required from external legal providers and police may be involved to determine the best way to secure evidence.

A record of what evidence has been gathered, stored and secured must be available as a separate log. Files and hardware must be securely stored, possibly in a designated offsite facility.

Data Protection and the UK GDPR – My Rights

In a school setting, personal data is stored and used for a variety of reasons. You may be a parent, carer, pupil, staff member, governor, visitor or anyone else who the school store data about. There are a number of categories of people, and many different types of data that is used in schools on a daily basis.

Whilst Privacy Notices set out details about why data may be collected, stored and used, there are some overriding principles that apply to every person (the Data Subject) when a school stores data. As Data Subjects, sometimes our consent is necessary for a school to process data about us. That might relate to photographs in school, reports in local press or similar. Consent is dealt with in the separate parts of the policy and can be accessed on the website or through the school office.

There are other occasions when data about us or our children may be used by the school to fulfil a legal obligation, a contract or some other lawful usage.

We all have other rights.

1. The right to rectification. Where data held about us is inaccurate, we have a right to apply for it to be amended and put right. This has to be done within one month, or within three months if it was complex. To do this we have to contact the data compliance manager within school, or the data protection officer. We have a right to complain if this is not done.

2. The right of access. This is a subject access request and is dealt with in more detail as part of the data protection policy. In essence, we have a right to see information about us that is classed as “personal data”. There is a separate process for us to make this request within school, and the school may ask us to clarify or be more specific about what kind of data we are asking for if there is a lot of it. Again, there is a one month timeframe for this that can be extended for three months in complex cases.

3. We have a right to erasure. This means that in certain circumstances we can ask for data about us to be permanently deleted. However, this can be limited if the data needs to be kept for some official or lawful purpose. The right to erasure sometimes occurs if we withdraw consent to a process.

4. We sometimes have the right to restrict processing. If we believe that data is inaccurate, and we have asked for it to be erased, we can ask the data processor and controller to stop any processing until the investigation into erasure or amendment has taken place.

5. There is also the right to data portability, this has little bearing in the school setting. Transfer of data for pupils is regulated by guidance from the Department for Education. Data about staff is part of HMRC contractual obligations. Data portability would usually apply to things like utility companies or bank accounts.

6. Individuals also have the right to object to personal data being used for marketing. Again, in the school setting this is likely to be very limited as the only marketing tends to be limited to school fetes, fairs and plays. Schools and academy trusts should not be sharing data with commercial third party entities to enable direct marketing of individuals. If this was the case, then an individual could object and ensure that the data was no longer used for that purpose.

7. As individuals we also have the right to ask that decisions are made about us on the basis of our data, rather than by an automated process. Again, any application of this in schools would be extremely limited. This tends to be regarding situations such as reference agency checks for loans and mortgages for example.

These rights are important and sit alongside the school or trust's legal obligations to manage our data properly.

Please also see the Privacy Notices and Data Protection Policy.

If you feel that any of the Rights set out here are not being managed properly, or if that information held of our files is inaccurate or should not be there or should be changed or amended, please do let us know.

There is a form to complete at the end of this document. By providing us with as much detail as you can about why you think we have got something wrong, or why we are holding information that we should not be keeping, it makes the process much simpler for you.

We will respond within 28 days of receiving the form, and we will give our reasons in writing for any decision we make.

When you get the decision you can accept it, and you need do nothing more. You can ask for a review by us and our Data Protection Officer, you can complain using our policy if you feel that we have not acted properly or you can make a referral to the Information Commissioner – whose details are found at https://ico.org.uk/ or by phone 0303 123 1113

Common to all privacy notices

The legal grounds for using your information

This is common for all personal and sensitive data we collect and process about staff, volunteers, pupils, parents, carers and any other individuals.

Some data is more sensitive than other types of data. These special categories are as follows: personal information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic information, biometric information, health information, and information about sex life or orientation.

Consent

The school will ask for consent to process data about you or a pupil. The type of data that is to be used, and how it is to be used will be specified on the consent forms.

You have the choice to opt in for certain types of data usage, and this is made clear. However, some data that is collected and processed in schools is not optional.

Legitimate interests

This means that the processing is necessary for legitimate interests except where the processing is unfair to you. The School relies on legitimate interests for many of the ways in which it uses information.

Specifically, the school has a legitimate interest in:

- Providing educational services to pupils
- Safeguarding and promoting the welfare of pupils and staff
- Promoting the objects and interests of the school
- Ensuring the efficient operation of the school
- Compliance with all relevant legal obligations of the school
- Keeping the whole school community informed about events, news and activities

Necessary for a contract

Information about individuals may be necessary to perform our obligations under our contracts.

For example, maintaining the school Management Information System database.

Legal obligation

Much of school life is governed by legal obligations to supply information to organisations such as the Department for Education or Local Authority or HMRC. We may also have to disclose information to third parties such as the courts, Disclosure and Barring Service or the police where legally obliged to do so.

Vital interests

For example, to prevent someone from being seriously harmed or killed.

Public interest

The School considers that it is acting in the public interest when providing education. Certain regulations, DfE and Local Authority, health and other guidance may require the school to process data in the public interest.

Legal claims:

The processing is necessary for the establishment, exercise or defence of legal claims. This allows us to share information with our legal advisors and insurers.

Your rights – what

What decisions can you make about your information?

From May 2018 data protection legislation gives you a number of rights regarding your information. Some of these are new rights whilst others build on your existing rights.

Your rights are as follows:

- you can ask what information we hold about you and be provided with a copy. Sometimes we are not able to share all the information, but this is set out in our Subject Access Policy
- if information is incorrect you can ask us to correct it
- you can ask us to delete the information that we hold about you or your child in certain circumstances. For example, where we no longer need the information;
- you can ask us to send you, or another organisation, certain types of information about you in a format that can be read by computer – this does not apply to pupil records as these are transferred by a DfE process called the Common Transfer File
- our use of information about you may be restricted in some cases. For example, if you tell us that the information is inaccurate we can only use it for limited purposes while we check its accuracy

If you disagree with any decision we make about your data you can use our complaints policy, you also have the right to make a complaint to the Information Commissioner, and sometimes to the Information Tribunal or through the court process. Our complaints policy is available on the website.

Common to all privacy notices

The legal grounds for using your information

This is common for all personal and sensitive data we collect and process about staff, volunteers, pupils, parents, carers and any other individuals.

Some data is more sensitive than other types of data. These special categories are as follows: personal information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic information, biometric information, health information, and information about sex life or orientation.

Consent

The school will ask for consent to process data about you or a pupil. The type of data that is to be used, and how it is to be used will be specified on the consent forms.

You have the choice to opt in for certain types of data usage, and this is made clear. However, some data that is collected and processed in schools is not optional.

Legitimate interests

This means that the processing is necessary for legitimate interests except where the processing is unfair to you. The School relies on legitimate interests for many of the ways in which it uses information.

Specifically, the school has a legitimate interest in:

- Providing educational services to pupils
- Safeguarding and promoting the welfare of pupils and staff
- Promoting the objects and interests of the school
- Ensuring the efficient operation of the school
- Compliance with all relevant legal obligations of the school
- Keeping the whole school community informed about events, news and activities

Necessary for a contract

Information about individuals may be necessary to perform our obligations under our contracts.

For example, maintaining the school Management Information System database.

Legal obligation

Much of school life is governed by legal obligations to supply information to organisations such as the Department for Education or Local Authority or HMRC. We may also have to disclose information to third parties such as the courts, Disclosure and Barring Service or the police where legally obliged to do so.

Vital interests

For example, to prevent someone from being seriously harmed or killed.

Public interest

The School considers that it is acting in the public interest when providing education. Certain regulations, DfE and Local Authority, health and other guidance may require the school to process data in the public interest.

Legal claims:

The processing is necessary for the establishment, exercise or defence of legal claims. This allows us to share information with our legal advisors and insurers.

Your rights – what

What decisions can you make about your information?

From May 2018 data protection legislation gives you a number of rights regarding your information. Some of these are new rights whilst others build on your existing rights.

Your rights are as follows:

- you can ask what information we hold about you and be provided with a copy. Sometimes we are not able to share all the information, but this is set out in our Subject Access Policy
- if information is incorrect you can ask us to correct it
- you can ask us to delete the information that we hold about you or your child in certain circumstances. For example, where we no longer need the information;
- you can ask us to send you, or another organisation, certain types of information about you in a format that can be read by computer – this does not apply to pupil records as these are transferred by a DfE process called the Common Transfer File
- our use of information about you may be restricted in some cases. For example, if you tell us that the information is inaccurate we can only use it for limited purposes while we check its accuracy

If you disagree with any decision we make about your data you can use our complaints policy, you also have the right to make a complaint to the Information Commissioner, and sometimes to the Information Tribunal or through the court process. Our complaints policy is available on the website.

Privacy notice for governors

Under data protection law, individuals have a right to be informed about how our trust and schools use any personal data that we hold about them.

School governors and trustees provide a vital role within our setting. Governors and trustees provide us with personal data and on occasion we share personal data with governors/trustees so that they can fulfil their obligations.

This privacy notice explains how we collect, store and use personal data about individuals who are governors or trustees.

The personal data we hold

We process data relating to those we appoint, or otherwise engage as governors or trustees, this may processing data about current office holders, or retaining data about those individuals who are no longer in role. Personal data that we may collect, use, store and share (when appropriate) about you may include, but is not restricted to:

- Contact details and copies of identification documents, including names, addresses, telephone numbers, email addresses, passport and birth certificates, visa details and other contact details;
- Date of birth, marital status and gender;
- Next of kin and emergency contact numbers;
- Bank account details (for the payment of expenses);
- Appointment information, including copies of right to work documentation, references and other information included in a CV or covering letter or as part of the appointment process;
- Qualifications and employment records, including work history, job titles, and professional memberships;
- DBS Certificate number and date of issue, prohibition from teaching and management checks, disqualification from childcare declaration form;
- Medical questionnaires and, where appropriate, information about an individual's health;
- Records of attendance at governing body and sub-committee meetings;
- Records and outcomes of any disciplinary, complaints and/or grievance procedures or other performance issues;
- Specimen signatures/signed mandates for delegated financial authority;
- Photographs and videos of participation in Schools' activities;
- CCTV footage captured by the Schools' CCTV system;
- **Vehicle details for those who use the Schools' car parking facilities.(if relevant or delete)**

Special Category data

Some of the information we hold is what is classed as special category data. Special category data includes any information concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, health, genetic or biometric data, and trade union membership. Where we need to process special category data we must fulfil an additional lawfully process, which is detailed below.

Why we use this data

The purpose of processing this data is to help us run the trust, including to:

- Enable governors and trustees to be paid for any expenses they have incurred;
- Enable appropriate organisational contact (for example, lists of governors and trustees for both internal and external use, including publication on the School's website);
- Allow for delegated financial authority (for example, cheque signing, bank mandates, contract signing);
- Facilitate safe appointment of governors and trustees, as part of our safeguarding obligations towards pupils;
- Support effective assessment and monitoring of governor and trustee performance;
- Inform our appointment and retention policies;
- Assist with management planning and forecasting, research and statistical analysis, including that imposed by law (such as diversity or gender pay gap analysis and taxation records);
- Arrange travel and accommodation for training courses, meetings, conferences, excursions, trips, visits and tours;
- Provide access to and use of the Schools' IT systems and to monitor use thereof, in accordance with the Schools' Acceptable Use Policy;
- Order goods and services, including appropriate insurance and professional advice for the Schools;
- Maintain relationships with alumni and the Schools' community;
- Meet the legal requirements of the Charity Commission and Companies House if necessary;
- Ensure security of the School site and including CCTV in accordance with the Schools' CCTV policy. IF YOU HAVE CCTV IF NOT DELETE

Our lawful basis for using this data

We only collect and use personal information about you when the law allows us to. Most commonly, we use it:

- When you have given us consent to use it in a certain way;
- To fulfil a contract we have entered into with you;
- To comply with a legal obligation;
- To carry out a task in the public interest.

Less commonly, we may also use personal information about you where:

- We need to protect your vital interests (or someone else's interests);
- We have legitimate interests in processing the data.

To process special category data we need an additional lawful basis. We will process special category data most commonly where:

- We have your explicit consent;

- The processing is necessary under social security or social protection law;
- We are processing it in the vital interests of an individual;
- We are providing health care or treatment under the responsibility of a health professional.

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you go about withdrawing consent if you wish to do so.

Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds which justify the school's use of your data.

Where we are processing data on a legal or contractual basis, if you choose not to share this data with us, we may not be able to carry out our obligations under our contractual relationship with you, or engage you as a governor.

Collecting this information

While the majority of information we collect from you is mandatory, there is some information that you can choose whether or not to provide.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

How we store this data

We create and maintain a personnel file for each governor in paper copy and/or electronic form on the Schools' computer system. The information contained in this file is kept secure and is only used for purposes directly relevant to you holding the position of governor.

Once your appointment as a governor or trustee has ended, we will retain this file and delete the information in it in accordance with our Retention of Records Policy, a copy of which is available by contacting the Data Protection Co-ordinator or the HR Manager at the Schools.

Data sharing

We do not share information about you with any third party, without your consent, unless the law and our policies allow us to do so.
Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about you with a number of organisations and agencies that may include (but is not limited to):

- All relevant local authorities – to meet our legal obligations to share certain information with it, such as safeguarding concerns;
- The Department for Education;
- Educators and examining bodies;
- Our regulator, the Independent Schools Inspectorate;
- Suppliers and service providers – to enable them to provide the service we have contracted them for;
- Central and local government;
- Financial organisations, such as HMRC;
- Our auditors;

- Survey and research organisations, including universities;
- Police forces, courts, tribunals;

.

Other Information

There is more information about how we manage, store and protect data in the Data Protection Policy on the website. This also includes details about how to access your data, how to contact the Information Commissioner or our Data Protection Officer if you have a query or concern about how data is being used or retained.

This notice is based on the Department for Education's model privacy notice for school governors, amended to reflect the way we use data in this school/trust.

This Notice

The Schools will update this Privacy Notice from time to time. Any substantial changes that affect your rights will be provided to you directly as far as is reasonably practicable.

Privacy Notice – Job Applicants

Introduction

When applying for a position in school, as an organisation we are the Data Controller. That means we have a statutory responsibility to explain how we collect, manage, use and store information about applicants.

You have a right to be informed about how our trust uses any personal data that we collect about you. This privacy notice, and our Data Protection Policy, explains our data usage when you apply for a job with us.

What information do we collect?

Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Name, address and contact details, including email address and telephone number
- Copies of right to work documentation
- References
- Evidence of qualifications
- information about your current role, level of remuneration, including benefit entitlements
- Employment records, including work history, job titles, training records and professional memberships

We may also request and collect, use, store and share (when appropriate) information about you that falls into "special categories" of more sensitive personal data. This includes, but is not restricted to:

- Information about race, ethnicity, religious beliefs, sexual orientation and political opinions
- Whether or not you have a disability for which the school needs to make reasonable adjustments during the recruitment process
- Photographs and CCTV images captured in school

We may also collect, use, store and share (when appropriate) information about criminal convictions and offences.

We may also hold data about you that we have received from other organisations, including other schools and social services, and the Disclosure and Barring Service in respect of criminal offence data.

Every school has statutory obligations that are set out in 'Keeping Children Safe in Education' and other guidance and regulations.

Why we use this data?

The school needs to process data to take steps at your request prior to entering into a contract with you. It may also need to process your data to enter into a contract with you.

The school needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check a successful applicant's eligibility to work in the UK before employment starts.

The school has a legitimate interest in processing personal data during the recruitment process and for keeping records of the process. Processing data from job applicants allows the school to manage the recruitment process, assess and confirm a candidate's suitability for employment and decide to whom to offer a job. The school may also need to process data from job applicants to respond to and defend against legal claims.

The school may process information about whether or not applicants are disabled to make reasonable adjustments for candidates who have a disability. This is to carry out its obligations and exercise specific rights in relation to employment.

Where the school processes other special categories of data, such as information about ethnic origin, sexual orientation, disability or religion or belief, this is for equal opportunities monitoring purposes.

For some roles, the school is obliged to seek information about criminal convictions and offences. Where the school seeks this information, it does so because it is necessary for it to carry out its obligations and exercise specific rights in relation to employment.

The school will not use your data for any purpose other than the recruitment exercise for which you have applied.

How do we use the data?

Your information may be shared internally for the purposes of the recruitment exercise. This includes members of the HR and recruitment team, shortlisting and interview panel members involved in the recruitment process (this may include external panel members), and IT staff if access to the data is necessary for the performance of their roles.

The school will not share your data with third parties, unless your application for employment is successful and it makes you an offer of employment. As well as circulating your application and related materials to the appropriate staff at the school, we will share your personal information for the above purposes as relevant and necessary with:

- your referees.
- Disclosure & Barring Service (DBS) in order to administer relevant recruitment checks and procedures.
- UK Visas & Immigration (UKVI) in order to administer relevant recruitment checks and procedures.
- Where relevant and as required for some posts, the Teacher Regulation Authority checks

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you would go about withdrawing consent if you wish to do so.

Automated Decision Making and Profiling

We do not currently process any personal data through automated decision making or profiling. If this changes in the future, we will amend any relevant privacy notices in order to explain the processing to you, including your right to object to it.

Collecting this data

As a school, we have a legal obligation to safeguard and protect our pupils and also staff, volunteers and visitors to our setting. We collect the data for specific purposes.

What if you do not provide personal data?

You are under no statutory or contractual obligation to provide data to the school during the recruitment process. However, if you do not provide the information, the school may not be able to process your application properly or at all.

Whenever we seek to collect information from you, we make it clear whether you must provide this information for us to process your application (and if so, what the possible consequences are of not complying), or whether you have a choice.

Most of the data we hold about you will come from you, but we may also hold data about you from:

Local authorities

Government departments or agencies

Police forces, courts, tribunals

How we store this data

The school takes the security of your data seriously. It has internal policies and controls in place to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by our employees in the proper performance of their duties.

We will dispose of your personal data securely when we no longer need it.

We keep applicant data for a period of up to 6 months if an applicant is not successful.

Successful applicants who secure a position then come within the employee/school workforce provisions.

Transferring data internationally

We do not share personal information internationally.

Your rights

You have a right to access and obtain a copy of your data on request;

You can:

- require the school to change incorrect or incomplete data;
- require the school to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing; and
- object to the processing of your data where the school is relying on its legitimate interests as the legal ground for processing.

If you would like to exercise any of these rights, please contact the school office. If you believe that the school has not complied with your data protection rights, you can complain to the Information Commissioner.

Complaints

We take any complaints about our collection and use of personal information seriously.

Our complaints policy deals with the different stages of any complaint, and how this is managed within school. You can also contact our Data Protection Officer or contact the Information Commissioner's Office:

Report a concern online at https://ico.org.uk/make-a-complaint/

Call 0303 123 1113

Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our data protection officer:

Our data protection officer is:

John Walker of J.A.Walker, Solicitor – info@jawalker.co.uk

However, our data protection lead has day-to-day responsibility for data protection issues in our school.

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact XXXXX

Privacy Notice – Pupil Data

Introduction

As a school we collect a significant amount of information about our pupils. This notice explains why we collect the information, how we use it, the type of information we collect and our lawful reasons to do so.

Why do we collect data?

We collect and use pupil data to:-

- Fulfil our statutory obligations to safeguard and protect children and vulnerable people
- Enable targeted, personalised learning for pupils
- Manage behaviour and effective discipline
- Monitor our effectiveness
- Comply with our legal obligations to share data
- Support pupils to fulfil their potential
- Keep pupils, parents and carers informed about school events and school news

Our Legal Obligations

We must make sure that information we collect and use about pupils is in line with the UK GDPR and Data Protection Act. This means that we must have a lawful reason to collect the data, and that if we share that with another organisation or individual we must have a legal basis to do so.

The lawful basis for schools to collect information comes from a variety of sources, such as the Education Act 1996, Regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013, Article 6 and Article 9 of the UK GDPR.

The Department for Education and Local Authorities require us to collect certain information and report back to them. This is called a 'public task' and is recognised in law as it is necessary to provide the information.

We also have obligations to collect data about children who are at risk of suffering harm, and to share that with other agencies who have a responsibility to safeguard children, such as the police and social care.

We also share information about pupils who may need or have an Education Health and Care Plan (or Statement of Special Educational Needs). Medical teams have access to some information about pupils, either by agreement or because the law says we must share that information, for example school nurses may visit the school.

Counselling services, careers services, occupational therapists are the type of people we will share information with, so long as we have consent or are required by law to do so.

We must keep up to date information about parents and carers for emergency contacts.

How we use the data

In school we also use various third party tools to make sure that pupils best interests are advanced. We also record details about progress, attainment and pupil development to support future planning and learning.

We use software to track progress and attainment.

We use data to manage and monitor pastoral needs and attendance/absences so that suitable strategies can be planned if required.

We use systems to take electronic payments for school meals. This includes financial software to manage school budgets, which may include some pupil data.

Data can be used to monitor school effectiveness, the impact of intervention and learning styles across groups of pupils as well as individual children.

We may use consultants, experts and other advisors to assist the school in fulfilling its obligations and to help run the School properly. We might need to share pupil information with them if this is relevant to their work.

We also use contact information to keep pupils, parents, carers up to date about school events.

What type of data is collected?

The DfE and government requires us to collect a lot of data by law, so that they can monitor and support schools more widely, as well as checking on individual schools effectiveness.

The categories of pupil information that the school collects, holds and shares include the following:

Personal information – e.g. names, pupil numbers and addresses

Characteristics – e.g. ethnicity, language, nationality, country of birth and free school meal eligibility

Attendance information – e.g. number of absences and absence reasons

Assessment information – e.g. national curriculum assessment results

Relevant medical information and social care

Information relating to SEND and health needs

Behavioural information – e.g. number of temporary exclusions

CCTV, photos and video recordings of you are also personal information.

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 pupil information we share with the department, for the purpose of data collections, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

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

The department 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-pupil-database-requests-received

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

Requesting access to your personal data

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact the school office.

You also have the right to:

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

If you have a concern about the way we are collecting or using your personal data, 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/

More information about Data Protection and Our Policies

How we manage the data and our responsibilities to look after and share data is explained in our Data protection Policy, and connected policies, which are also available on our website.

If you feel that data about your child is not accurate, or no longer needed please contact the schools office. Our complaints policy explains what to do if there is a dispute. Subject Access Requests are dealt with by the specific policy on the website.

Privacy Notice School Workforce

This privacy notice explains how we collect, process and manage information for the school workforce. That includes employed members of staff, volunteers, including trustees and governors, trainee teachers, apprentices and work experience/workplace placements.

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

- personal information (such as name, employee or teacher number, national insurance number)
- special categories of data including characteristics information such as gender, age, ethnic group
- contract information (such as start dates, hours worked, post, roles and salary information)
- work absence information (such as number of absences and reasons)
- qualifications (and, where relevant, subjects taught)
- medical information
- other personal information
- references

We use and share information to comply with statutory, regulatory, practice and contractual obligations. These may include, but are not limited to:-

- improving the management of workforce data across the sector
- enabling development of a comprehensive picture of the workforce and how it is deployed
- pay salaries and pension contributions
- informing the development of recruitment and retention policies
- allowing better financial modelling and planning
- enabling ethnicity and disability monitoring
- supporting the work of the School Teachers' Review Body
- comply with guidance such as 'Working Together' and safeguarding obligations
- facilitating good governance
- internal reviews and quality monitoring
- CPD and staffing issues

If we are required to comply with other legal obligations not listed above we will share data only when it is lawful to do so.

The lawful basis on which we collect and process this information

We must make sure that information we collect and use about pupils is in line with the UK GDPR and Data Protection Act. This means that we must have a lawful reason to collect the data, and that if we share that with another organisation or individual we must have a legal basis to do so.

The lawful basis for schools to collecting and processing information comes from a variety of sources, such as the Article 6 and Article 9 of the UK GDPR, the Safeguarding of Vulnerable Groups Act 2006. We also have obligations to organisations such as HMRC and the Department of Work and Pensions.

Collecting this information

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

Storing this information

We hold school workforce data for in accordance with our HR and Retention Policy

Who we share this information with

We may share this information with organisations such as:

- our local authority
- the Department for Education (DfE)
- Safeguarding and protection for children and vulnerable adults
- Payroll services
- Legal Advisers
- Insurance providers
- HMRC
- Teacher Pension Scheme and the Local Government Pension Scheme (and other pension providers
- Health professionals

[Settings need to amend and extend this list to include all other parties with whom they regularly share information. For example, academy chains / federations / Multi Academy Trusts (MATs). Once stated you also need to explain why you share the data and what makes it lawful below]

Why we share school workforce information

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

Local authority

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

Department for Education (DfE)

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

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

Data collection requirements

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

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

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

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

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

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

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

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

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

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

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information please see the Subject Access Request information that is on the website.

You also have the right to:

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

More details about how we use and manage data can be found in the 'Data Processing Notices – Common Principles and Processes', the Data protection Policy and other relevant polices for the School Workforce on the website.

Consent Guide

ALSO IN THE DATA PROTECTION POLICY KEY ELEMENTS – SCHOOLS MAY WISH TO HAVE AN ANNEX THAT USES THIS OR SEPARATE DOC RE CONSENT

Consent

As a school we will seek consent from staff, volunteers, young people, parents and carers to collect and process their data. We will be clear about our reasons for requesting the data and how we will use it. There are contractual, statutory and regulatory occasions when consent is not required.

We may process personal and sensitive data without consent if another provision applies.

Consent is defined by the GDPR as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

We may seek consent from young people also, and this will be dependent on the child and the reason for processing.

Consent and Renewal

On the school website we have 'Privacy Notices' that explain how data is collected and used. It is important to read those notices as it explains how data is used in detail.

Obtaining clear consent and ensuring that the consent remains in place is important for school. We also want to ensure the accuracy of that information.

When a pupil joins us, part of the process is to seek consent. This information is retained on the pupil file. If there are any changes, please inform us.

For Pupils and Parents/Carers

On arrival at school you will be asked to complete a form giving next of kin details, emergency contact and other essential information. We will also ask you to give consent to use the information for other in school purposes, as set out on the data collection/consent form.

Pupil consent procedure

Where processing relates to a child under 13 years old, school will obtain the consent from a person who has parental responsibility for the child.

Pupil's may be asked to give consent or to be consulted about how their data is obtained, shared and used in certain situations.

Withdrawal of Consent

Consent can be withdrawn, subject to contractual, statutory or regulatory constraints.

Where more than one person has the ability to provide or withdraw consent the school will consider each situation on the merits and within the principles of GDPR and also child welfare, protection and safeguarding principles.

Please complete the appropriate form which is available on the website.

This must be returned to the school the pupil attends.

Consent Withdrawal Form - Adult

Please complete and deliver this form to the school office with your signature.

Please note that as a school we may have contractual, statutory and/or regulatory reasons why we will still process and hold details of a pupil, parent, staff member, volunteer or other person.

Where two parents share parental responsibility, or where PR is shared and the pupil is capable of expressing a view and there is conflict between the individuals the process of withdrawing consent will be subject to an evaluation and discussion to enable a decision to be reached that is considered to be in the pupil's best interests.

Withdrawal of consent for an individual

I, …… , withdraw consent for …….. (SCHOOL) to process my personal data. I withdraw consent to process my personal data for the purpose of …… , which was previously granted.

Signed:

Date:

Received by school

School staff member:

Dated:

Actions:

Consent Withdrawal Form – on behalf of Pupil

Please complete and deliver this form to the school office with your signature.

Please note that as a school we may have contractual, statutory and/or regulatory reasons why we will still process and hold details of a pupil, parent, staff member, volunteer or other person.

Where two parents share parental responsibility, or where PR is shared and the pupil is capable of expressing a view and there is conflict between the individuals the process of withdrawing consent will be subject to an evaluation and discussion to enable a decision to be reached that is considered to be in the pupil's best interests.

We may need to seek identification evidence and have sight of any Court Order or Parental Responsibility Agreement in some cases to action this request. If this is the case a senior member of school staff will discuss this with you.

Withdrawal of consent on behalf of a pupil

I, …… , withdraw consent in respect of ……. (Pupil Name) for ……. (SCHOOL) to process my personal data. I withdraw consent to process their personal data for the purpose of …… , which was previously granted.

I confirm that I am …….. (Parent/Carer) and that I have parental responsibility for the pupil.

Signed:

Date:

Received by school

School staff member:

Dated:

Actions:

Complaint Policy Insert

GDPR and DPA Complaints

All Staff must be aware of the complaints process. All complaints should be directed to the Data Protection Compliance Manager / Data Protection Officer. If any member of staff is aware that a person wishes to complain they should direct the person to the school website and complaints policy and form.

ADD TO POLICY

Complaints Manager/Data Protection Compliance Manager / Data Protection Officer is responsible for dealing with all complaints in line with this procedure.

The school complaints policy sets out the complaints process. This will be the basis for dealing with Data Protection Complaints and appeals. A written outcome will be provided.

If the school does not comply with a Subject Access Request within 1 month (subject to any extension), or refuses all or part of the request, written reasons will be provided, setting out the principles for the refusal.

If you feel that the school have not dealt with your matter satisfactorily you can complaint to the Information Commissioner

By post:
Customer Contact
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
SK9 5AF

Or by email: casework@ico.org.uk

More information is on the ICO website www.ico.org.uk/

COMPLAINTS POLICY WILL NEED TO BE REVIEWED AND ADDITIONS MAY BE NEEDED TO CLARIFY AND CONFIRM THE PROCESS

CCINS
CONFIDENTIALITY POLICY
&
CONFIDENTIALITY AGREEMENTS

Aim

To ensure that confidentiality and Data Protection Compliance are a natural part of good practice. To provide all staff, governors and others in school clear, unambiguous guidance as to their legal and professional roles. To make certain that the procedures throughout the school can be easily understood by pupils, parents/carers and staff.

Rationale

Schools hold a lot of confidential information about children, staff and sometimes parents and carers. Whilst it is important that we continue to develop positive ways to use that information, we all recognise that it is our responsibility to use, hold and safeguard information received.

The school is mindful that it is placed in a position of trust by all stakeholders and there is a general expectation that a professional approach will be used in all matters of confidentiality. Our obligation to comply with the Data Protection Act 2018, the GDPR and other legislation and statutory guidance underpins our management of data.

Objectives:

- To provide consistent messages in school about handling information about children and adults once it has been received.
- To foster an ethos of trust within the school.
- To ensure that staff, governors, volunteers, students, parents, and pupils are aware of the school's confidentiality policy and procedures.
- To reassure pupils that their best interests will be maintained.
- To encourage pupils to talk to their parents and carers.
- To ensure that pupils and parents/carers know that school staff cannot offer unconditional confidentiality.
- To ensure that if there are child protection issues then the correct procedure is followed.
- To ensure that confidentiality is a whole school issue and that everyone understands their personal responsibilities.

Guidelines

- All information about individuals is private and should only be shared with those staff that have a need to know.
- All social care, medical and personal information about a child should be held in a safe and secure place which cannot be accessed by individuals other than school staff.
- The school continues to actively promote a positive ethos and respect for the Individual.
- The Safeguarding Policy will be applied, and monitored by appropriate school personnel.
- All children and adults have a right to the same level of confidentiality irrespective of gender, race, religion, medical concerns, and special educational needs.

Day to Day Practice

Confidentiality is a whole school issue. Even when sensitive information appears to be widely known it should not be assumed by those immediately involved that it is appropriate to discuss or share this information further.

Health professionals have their own code of practice dealing with confidentiality. Staff should be aware of children with medical needs and the class should be accessible to staff who need that information but not on general view to other parents/carers and children.

Information about children will be shared with parents and carers but only about their child. **Parents should not have access to any other child's books, and assessment information at any time especially at parents evening.**

All personal information about children including social care records should be regarded as confidential. It should be clearly understood by those who have access to it, and whether those concerned have access to all, or only some of the information.

Information regarding health reports such as speech therapy, medical reports, SEN reports, SEN minutes of meetings and social care minutes of meetings and reports will be circulated in envelopes / files and once read should be returned for secure filing. CPOM's and Egress Secure Email is used to safely share information electronically.

In all other notes, briefing sheets etc. a child should not be able to be identified. Addresses and telephone numbers of parents and children will not be passed on except in exceptional circumstances or to a receiving school.

Staff should exercise prudence and consider the dignity of individuals during conversations on the school site, for example in the staff room, particularly if non -members of staff are present and in the presence of children.

Non-members of staff, for example, students and voluntary helpers, will be asked to follow the principles of the confidentiality policy and sign a confidentiality agreement.

Governors

Governors need to be mindful that from time to time issues are discussed or brought to their attention about staff and children. All such papers should be marked as confidential.

These confidential papers should be destroyed after use.

Governors must observe complete confidentiality when asked to do so by the governing body, especially in relation to matters concerning individual staff, pupils or parents.

Governors will sign a confidentiality agreement annually.

Although decisions reached at governors' meetings are normally made public through the minutes or otherwise, the discussions on which decisions are based should be regarded as confidential.

Governors should exercise the highest degree of prudence when discussion of potentially contentious issues arises outside the governing body.

Monitoring and Evaluation

The policy will be reviewed as part of the schools monitoring cycle.

Conclusion

CCIN School has a duty of care and responsibility towards pupils, parents/carers, and staff. It also needs to work with a range of outside agencies and share information on a professional basis. The care and safety of the individual is the key issue behind this document.

Policy agreed by governors and shared with staff, volunteers and the school community.

CCIN School

Governor - Confidentiality Agreement

First of all, thank you for volunteering to be a Governor of this school.

Your help and support in this role is greatly appreciated. In this role you are supporting the life of this school. This role carries certain responsibilities on your part including the requirement to be confidential about school matters. By signing this agreement, you agree to uphold CCIN School's Confidentiality Policy.

This means you will not share pupil / staff information with anyone other than those who are directly involved.

Examples of confidential information are (but not limited to):

- Information about staff and pupils.
- Information about actions of the Governing Body that are not published In Governing Body minutes.
- Information accessed by 'privilege' e.g. notices on staff noticeboard.
- Information about future school plans / actions than have not been disclosed to parents.

I understand that I may have access to confidential information and that it is my responsibility to maintain the integrity of this information and to keep it private. I further understand that disclosure of confidential information may result in termination of my membership of the Governing Body.

If I breach confidentiality I understand that I may be in breach of the Data Protection Act 2018 and could face external sanctions.

Name of Governor	
Signature of Governor	
Date	
School Representative	
Signature of School Representative	
Date	

CCIN School
Volunteer - Confidentiality Agreement

First of all, thank you for volunteering to be a helper at this school. Your help and support in this role is greatly appreciated. In this role you are supporting the life of this school. This role carries certain responsibilities on your part including the requirement to be confidential about school matters.

By signing this agreement, you agree to uphold CCIN School's Confidentiality Policy.

This means you will not share pupil / staff information with anyone that breaches confidentiality.

Examples of confidential information are (but are not limited to):

- Information about staff, pupils, and events that occur in school.

For example, a parent who knows you are a helper at the school may ask you how their child is getting on (e.g. academically / behaviour). To prevent a misunderstanding, it would be better to advise the parent to speak to the class teacher.

- Information accessed by 'privilege' e.g. notices on staff noticeboard /conversations
- If you see something in school that concerns you, please discuss the matter with the head teacher.

I understand that I may have access to confidential information and that it is my responsibility to maintain the integrity of this information and to keep it private. I further understand that disclosure of confidential information may result in me no longer being required to be a volunteer.

If I breach confidentiality I understand that I may be in breach of the Data Protection Act 2018 and could face external sanctions.

Name of Volunteer	
Signature of Volunteer	
Date	
School Representative	
Signature of School Representative	
Date	

CCIN School
Student/Work Experience - Confidentiality Agreement

Please read the school's Confidentiality Policy.

This work placement / experience carries certain responsibilities on your part including the requirement to be confidential about school matters.

By signing this agreement, you agree to uphold CCIN School's Confidentiality Policy. This means you will not share pupil / staff information with anyone that breaches confidentiality.

Examples of confidential information are (but are not limited to):

- Information about staff, pupils, and events that occur in school.
- Information accessed by 'privilege' e.g. notices on staff noticeboard /conversations.
- If you see something in school that concerns you, please discuss the matter with the head teacher.
- You must never use information about individual children outside the school without parental permission (photographs/names).

I understand that I may have access to confidential information and that it is my responsibility to maintain the integrity of this information and to keep it private. I further understand that disclosure of confidential information may result in me no longer being able to complete my placement as a student and that this breach may be reported to those who arranged the placement or my course leader.

If I breach confidentiality, I understand that I may be in breach of the Data Protection Act 2018 and could face external sanctions.

Name of Student	
Signature of Student	
Date	
School Representative	
Signature of School Representative	
Date	

Information Security Policy

Aims of the Policy

1. To set out examples of good practice for the governance of personal data and information in all its forms, balancing the need to process and manage data set against risk of data breach.

2. To maintain and improve the security of our systems and the quality of our data by improving the data capability and awareness of our staff, students, and other users of the CCINS data or computing and networking facilities and ensuring they are supported by appropriate tools and processes.

3. To ensure that appropriate technical and organisational measures are in place to prevent unauthorised access, damage or interference to and/or with information, IT assets and network services

4. Both as an organisation and for individuals who process our data to ensure that that it we are aware of, and comply with, the relevant legislation as described in this and the other information governance and IT Policies

5. To describe the principles of Information Security to members of staff, pupils and other authorised persons and to explain how these will be implemented by the School/trust;

6. To develop and maintain a level of awareness of the need for information security to be an integral part of the conducting of school/trust business and ensuring that everyone understands their individual and collective responsibilities in this respect;

7. To Protect personal data and other information held on our systems.

8. The impact of this policy will be to improve security and data management standards.

9. The terms ‘personal data’ and ‘information’ are used interchangeably in this policy, as are ‘information security’ and ‘cybersecurity’.

This policy does not specifically address issues of privacy or personal data protection, although good data management and security are essential for compliance with data protection laws. Concerning privacy and data protection, the Data Protection Policy, Privacy Notices IT Usage, Bring your Own Device (DELETE OR INCLUDE YOUR OWN POLICIES AS APPROPRIATE) take precedence.

This policy will be regularly reviewed and updated to ensure it remains current.

Relevant Legislation

There are many laws and regulations governing how information is handled, including:

- Common law in relation to duties of confidentiality;
- Regulation of Investigatory Powers Act 2000
- Data Protection Act 2018
- Human Rights Act 1998
- Protection of Children Act 1999
- Freedom of Information Act 2000
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988;

- Health and Safety at Work Act 1974;
- Theft Act 1978;
- Indecent display (Control) Act 1981
- Obscene Publications Act 1984
- UK General Data Protection Regulations 2018 (UK GDPR)

Personal Data

For purposes of this Policy, "Personal Data" means information that can identify an individual and is set out in the Data protection policy.

It is important to note that some data is more sensitive and must be treated with greater care an understanding about the basis to process this sensitive data that includes:

- personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs
- trade-union membership
- genetic data, biometric data processed solely to identify a human being
- health-related data
- data concerning a person's sex life or sexual orientation

Implementation of this Policy

- Staff and authorised persons awareness will be managed by training and induction
- Regular testing of the our IT and physical data safeguards
- Evaluating the ability of each of our third party service providers to implement and maintain appropriate security measures for the Personal data to which we have permitted them access; and requiring such third party service providers by contract to implement and maintain appropriate security measures
- Reviewing the scope of the security measures at least annually, or whenever there is a material change in our practices that may implicate the security or integrity of records containing personal data
- Conducting an annual training session for all relevant people who have access to Personal data on the elements of the policy, and keeping a record of attendees.

Storage of Information

The amount of personal data collected, and the time period for retention, should be limited to that amount reasonably necessary to accomplish our legitimate purposes, or necessary for the organisation to comply with other legal requirements, regulatory obligations and relevant advice from the Department for Education.

Systems to store data, including material from emails, will be in place to comply with our Record of Processing Activities. These may be physical or electronic/digital records.

Examples that set out more detail about good information management and security will be shared with staff and authorised persons. (see Twenty Tips for Staff – Toolkit Section 10) and Schedule 1 to this policy.

Physical Records — Records containing personal data (as defined above) must be stored appropriately, and records containing sensitive data should be stored in locked facilities, secure storage areas or locked cupboards or offices.

Electronic Records — To the extent technically feasible, the following security protocols must

be implemented:

Secure user authentication protocols including:

- control of user IDs and other identifiers
- a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices
- control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect
- restricting access to active users and active user accounts only
- blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system

Secure access control measures that:

- restrict access to records and files containing personal data to those who need such information to perform their job duties; and
- assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls

Encryption of the following:

- all transmitted records and files containing personal data that will travel across public networks, and encryption of all data containing personal data to be transmitted wirelessly
- all personal data stored on laptops or other portable devices
- reasonable monitoring of systems, for unauthorised use of or access to personal data;
- For files containing personal data on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal data
- Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.

Access to Information

Access to records containing personal data shall be restricted to current employees or approved persons who are reasonably required to know such information in order to support the school/trust's objectives.

Records containing Personal data shall only be removed from the site with specific authorisation from a relevant member of SLT or as part of an employee's job description.

Staff and approved persons who have access to personal data will logoff their computers when not in use for an extended period of time.

During short periods of inactivity, these staff and approved persons will either lock their computers at the operating system level or ensure that no unauthorised person can gain access - this is of particular importance for computers or devise in classrooms or teaching areas if the device or computer is left unattended at any point.

Visitors' to the site where personal data is stored shall not be permitted to visit any area of the premises that contains personal data unless they are escorted by a school/trust employee.

Employees are encouraged to report any suspicious or unauthorized use of Personal data.

Transmission of Information

To the extent technically feasible, all records and files containing personal data which are transmitted across public networks or wirelessly must be encrypted or secured.

Staff and authorised persons are prohibited from keeping open files containing sensitive personal data on their desks or in their work or teaching areas when these are unattended by a member of staff or authorised person.

At the end of the school day, all files and other records containing personal data must be secured in a manner consistent with this policy.

Disposition/Destruction of Information

Paper and electronic records containing personal data must be disposed by a secure and approved method that is understood by all staff or authorised persons.

Any temporary or permanent staff who leave the school/trust must return all records containing personal data, in any form, which may at the time of such termination be in the former persons' possession (including all such information stored on laptops or other portable devices or media, and in files, records, work papers, etc.)

Training

A copy of this Policy will be distributed to each employee or authorised person, (as well as visitors and suppliers as appropriate), who will have access to personal data. All such persons shall, upon receipt of the Policy, acknowledge in writing that he/she has received, read and understood it.

When the Policy is first issued, there will be training of employees and temporary employees who have access to personal data on the detailed provisions of the policy. All employees shall be retrained regularly.

All attendees at such training sessions are required to certify their attendance at the training and their familiarity with the company's policy and procedures for the protection of personal data.

Breaches

Breaches of the policy will be investigated and may be met with disciplinary action up to and including termination of employment. The nature of the disciplinary measures will depend on a number of factors including the nature of the violation.

Any suspected breach should be reported immediately and the 'Breach and Non Compliance' procedure is to be followed.

Third Parties

The contents of this Policy will apply to third parties who are intended to receive and process personal data.

Exceptions

Any exceptions to this policy require prior written authorisation and approval from the

headteacher/CEO.

Approved by…….

Dated……..

Review data…….

Schedule 1

Good Practice Guise

The Data Protection Act 2018 sets out 6 principles concerning personal data, requiring that it must:

- Be processed fairly and lawfully;
- Be processed for specified purposes;
- Be adequate, relevant and not excessive;
- Be accurate and up-to-date;
- Not be kept for longer than necessary for the specified purpose;
- Be processed in accordance with the rights of data subjects;
- Be protected by appropriate practical and organisational security;
- Not be transported (including electronically) outside the European Economic Area without ensuring protection for the data is at least as good as in the EEA.
- Parents and staff must be made aware that the information they give us may be recorded, may be shared in order to provide appropriate education and care, and may be used to support audit and other work to monitor the quality of education and care provided.

To do this we are all responsible for personal data when it is in our control.

Keeping Records Secure

All records that include student / staff identifiable information will be stored appropritately which may include securely in locked filing cabinets, password protected electronic databases or another form of restricted access storage when not in use depending on the sensitivity of the information contained in the records.

Employees are expected to take appropriate measures to ensure the security of personal data at all times, including keeping records secure attending meetings or removing records from site to work on at home.

Access to computer equipment should be restricted by closing windows and doors when the room / office is not in use. Computer screens should be always be locked (Ctrl, Alt and Del) if being left switched on and unattended.

Access will be afforded on a “need to do” basis, and access of leavers removed promptly.

So far as is reasonably practicable only authorised persons will be admitted to rooms that contain servers or provide access to data.

Equipment and paper files must not be left on view in any public setting.

Computer monitors should be positioned in such a way that information stored or being processed cannot be viewed by unauthorised persons or members of the public.

Documents or files containing personal identifiable information should be saved onto a shared network, with appropriate security protection, and not onto the C: Drive.

All school-owned ICT equipment, including software, should be recorded and security marked.

Users must not make, distribute or use unlicensed software or data on site.

Mobile devices (e.g. laptops, memory sticks, etc.) must be encrypted for all sensitive, personal or confidential data. (see appendix 2)

Passwords

Passwords must not be shared with other members of staff under any circumstances.

Passwords should not be written down and/or left on display or be easily accessible.

Passwords should be “complex”, comprising a combination of letters and numbers (preferably upper and lower case) and should be changed frequently.

The “remember password” feature should never be used.

Staff are encouraged to password protect any personal files, in particular those that contain potentially embarrassing information about an individual or an organisation.

Transfer / Sharing of Personal Data and/or Confidential Information

The Data Protection Act 2018 should be considered at all times when recording, sharing, deleting or withholding information.

Sensitive information must not be shared unless the person is authorised to receive it.

Email and Electronic sharing

Any transfers of confidential information should be secure and the method risk assessed.

For electronic information transfers encrypted software should be used.

When information is requested by telephone it is important to:

- Ask the caller to confirm their name, job title, department and organisation and verify this by returning their call via their organisation’s switchboard;
- Confirm the reason for the request;
- Be satisfied that disclosure of the requested information is justified;
- Place a record on the student / staff file noting the name of the person disclosing the information, the date and time of the disclosure, the reason for the disclosure, who authorised it (if applicable) and the recipient’s details..

When sending personal or sensitive information by post:

- Check the name, department and address of the intended recipient;
- Use a robust envelope, clearly marked “**PRIVATE & CONFIDENTIAL To be opened by the addressee only**”;
- Information to a service or department within the Local Authority should be sent using the internal post system;
- If the public post system is to be used a return address must be recorded on the outside of the envelope, and recorded delivery should be used if the information is considered to be highly sensitive.

EMPLOYEE ACKNOWLEDGEMENT FORM

I have received, read and understand the Information Security Policy. I understand that it is my responsibility to comply with it.

Printed name: _____
Signature:_____
Date:_____

A SECURITY BREACH is any incident or activity that causes, or may cause, a break down in the availability, confidentiality or integrity of the physical or electronic information assets of School/Trust.

Cavendish Close Infant and Nursery School Records Management Policy

Management of records is a legal obligation (Section 46 of the Freedom of Information Act 2000). By ensuring that our records are well managed and controlled we can provide a better service to staff, pupils, parents/carers and others. The legal and regulatory obligations from many sources rely on effective record management. Information management is also a part of the IT strategy, Data Protection and UK GDPR compliance obligations. This policy provides a framework that covers records management in the trust and the academies. It covers:

• Scope

• Responsibilities

• Relationships with existing policies

1. Scope

1.1 This policy applies to all records created, received or maintained by staff of the trust/school, whether centrally or in individual schools, in the course of carrying out its functions.

1.1 Records exist in the trust/school and in schools and originate from a variety of sources. Trust staff will create some. Others are provided by parents/carers and pupils, others are shared with the trust and its schools by external professionals. The policy applies to all records and the management of the records in the trust and its schools. See Appendix 1 for examples of records in the trust/school and schools.

1.2 Records may be hard copy, electronic, digital, images, audio recordings or any other source that can be viewed, heard or interrogated. They may relate to individuals, financial planning, contracts, commercial organisations, public authorities or charitable organisations. Some will include personal data about individuals.

1.3 How the trust and schools use, maintain and manage records will be dependent on the purpose, origin and source of the records. Other policies will govern this in many instances.

1.3 Some records will be retained for historical and archiving purposes.

2. Responsibilities

2.1 The trust/school has a corporate responsibility to maintain, use, store and delete its records to comply with regulatory requirements. The person with overall responsibility for this policy is the Chief Executive Officer/Headteacher, and this will be delegated to individuals in each school.

2.2 Good record management practice will be the responsibility of all staff. Individual responsibility will be determined by job description and practice. A senior leader (head, principal or head of school) will also monitor compliance with this policy at least annually.

2.3 Individual staff and employees must ensure that records for which they are responsible are accurate and are maintained and disposed of in accordance with the trust's policies and records management guidelines.

3. Relationship with existing policies

This policy has been drawn up within the context of:

- Freedom of Information policy
- Data Protection policy
- Information Security policy
- IT security and use polices
- Records retention policy/guidelines
- and with other legislation or regulations (including audit, equal opportunities and
- ethics) affecting the trust and schools.

Signed……..

Dated……..

Appendix 1

The trust/school and schools keep a wide variety of records that may include (but are not limited to):

Students

- Personal information
- Parent/carer contact information
- School reports
- Behaviour logs
- Exam and testing outcomes – internal and external
- Child protection information
- Allegations of a child protection nature made against a member of staff (including unfounded allegations)
- Attendance – attendance registers, authorised absence correspondence
- SEND – reviews, advice to parents/carers, accessibility strategy
- Pupil Premium / Sixth Form Bursary – evidence of eligibility
- Free School Meals eligibility
- Services and Pupil Premium eligibility
- LAC status
- Medical – Individual Health Plans, first aid records
- Biometric records

Management of the Trust and Schools

- Trust and Governing Board records - agendas, minutes, resolutions, reports
- Trustee and Governors personal details
- Declarations of Interests
- CPD and training
- Statutory Documents for Companies House
- Accounts and Trust Report
- School Development Plans and School Improvement plans
- Leadership meetings, minutes and actions
- Admission details
- School visitor logs
- Health and Safety Records
- Fire Risk Assessments
- Risk Assessments
- Social Media
- Newsletters and external communication records

Human Resources

- Job Descriptions
- Application forms
- Personnel files for all staff – including personal contact details
- Appraisals
- Performance reviews
- Employment suitability checks
- Contracts of employment

- Records of Disciplinary and Grievances Process
- Allegations and LADO referrals
- Referrals to the TRA and/or DBS
- Payroll and pensions – maternity/paternity pay, family leave records,

Financial Management

- Budgets and Funding details as required by the Funding Agreement, Academies Financial Handbook and Company Law
- Risk Management and Insurance – employer's liability insurance certificate
- Asset Management Records
- Asset Register
- All necessary financial records
- Contracts
- Contract Management and Procurement
- School Payment and Meals Management
-

Property Management

- Property Management
- Condition Surveys
- Hire agreements
- Maintenance – log books, warranties and contractor information
- Health and safety information

Curriculum & Attainment

- Teaching and learning planning
- Timetabling and resource planning
- Prospectus and Website
- Statistics and evidence of learning outcomes, targets
- Pupil work records
- Trip and visit record

External Records

- Central Government and Local Authority
- Local Authority – census returns, attendance returns
- Central Government – returns made to DfE/ESFA
- Ofsted
- Referrals to third party agencies
- Legal action involving the trust and schools
- ICO action
- Enquiries and investigations by external bodies

Information Sharing – Good Practice

Many school policies refer to data sharing between schools and individuals or partner organisations. Data must be shared in compliance with the Data Protection Act 2018 and UK GDPR. Other statutory obligations and official guidance need to be considered when dealing with data sharing.

The DfE's Guidance on Information Sharing for Practitioners 2018 has a summary of these obligations.

Overarching all policies should be a framework for information sharing which is driven by the key principles set out by the Government.

1. Necessary and proportionate

Data should only be shared with any third party, internally or externally, on the basis that it is proportionate to the need and fulfils the objective of the legitimate request. Different levels of risk will require individuals to make decisions on a case-by-case basis. Enough information should be provided to fulfil the policy or obligation.

2. Relevant

Relevant information should be shared with those who need it. This should be limited and principles of data minimisation should be applied. Depending on the individual request, will determine the amount of information that is required.

3. Adequate

Information supplied should be fit for purpose and should be the right quality for the recipient to understand and be able to act upon it, rely upon it or understand it. Too little information is as dangerous as too much.

4. Accurate

Staff should be mindful to provide information that is as accurate as possible. This may require checking on school systems prior to giving information out. Reminders should be sent to parents, carers and staff about updating information over the course of the academic year.

5. Timely

Information may be required on an urgent basis. Taking account of potential risks of not sharing information may lead to greater risks for pupils, or indeed adults. Sharing information needs to be on a timely basis, and on occasion requesters may have to be informed that a response will not be immediate. Realistic timescales should be shared.

6. Secure

Individuals must follow their own organisation's security measures. Processes for sharing personal and sensitive data should be applied in every case. Guidance around delivering information should be on a scale, the more sensitive the information the more care must be taken in sharing it.

7. Recording

Decisions in respect of information sharing should be recorded. Clearly the more sensitive the information being shared the more detail about why it was shared, who was shared with, how it

was shared and the basis for sharing need to be in place. Day-to-day conversations do not need to be shared, emails and other correspondence may provide a suitable record if they have enough detail. Information should not be stored for longer than necessary and should be subject to retention policies and timelines.

When sharing information, it is important to understand the legal basis under UK GDPR. In many instances in schools, there is a legal duty to process information. However, it may also be by consent or part of a contract or as part of a public task. Sharing safeguarding and information that prevents or protects individuals from significant harm or requires immediate medical treatment to save and protect are dealt with under the category of vital interests.

Information requests from the Police, Social Care or Court Service need to be approached in the same way and properly considered about what information can, or could not be shared.

Information should be shared in accordance with policies.

If there is any question about the nature of information to be shared, or reasons for sharing, or not sharing, advice should be taken from the UK GDPR lead in school and the Data Protection Officer.

Consent Forms

PLEASE NOTE THIS IS NOT A DEFINITIVE LIST OF CONSENT. THIS IS ONLY APPLICABLE FOR GDPR ISSUES – some schools choose to have other types of consent for climbing frame use, snow ball fights, PE and activities.

IT fair usage polices, IT security policies, medical and pastoral information, discipline, behaviour and similar school management polices and arrangements are not covered within this list. Home School Agreement or Pupil Agreements must be considered separately.

THESE ARE NOT CONSIDERED AS PART OF GDPR COMPLIANCE

Photographs, Video and Media

	Yes	No
May we use your child's photograph in printed publications that we produce for promotional purposes such as a prospectus or on project display boards?		
I give consent for my child's image to be used on the school website and school social media		
May we record your child's image on video or webcam?		
I give consent for my child and their details to appear in the media. (for example in the local press, radio or TV)		
Are you happy for your child to appear on Social Media sites used by the school/college e.g. Twitter and Facebook ?		
I give consent for my son or daughter to be included in any school or class Yearbook and other mementos on leaving the school (if applicable)		
Do you consent for your son or daughter's name to be released for publication such that they may be identified as an individual or as part of a small group? For example raising money for charity that is recognised in the local media.		
I give consent for my son or daughter to be photographed for school group photos, that may be bought by other families who have children in the photo.		
I give consent for a professional photographer to take photographs and release to my family for sale? The photographer would have possession of the photos on their equipment, not school equipment.		
Are there any reasons why your child cannot participate in events and performances that may be recorded or photographed and shared with the school community? If yes please contact school to explain your concerns.		

Medical

Schools must have the right policy for children with medical conditions in schools.

Consent from the parent/carer is essential before referring to the School Health Nursing Service, unless the referral is a self-referral from a young person deemed competent.

You may wish to include this request as part of the consent and data collection forms.

This should not replace your existing collection arrangements or policies

Doctors Practice	
Doctors Name	
Telephone Number	
Does your child suffer from any health problems, if so please give details. (Please indicate any special treatment)	
Permission to contact Doctor	Yes/No (Please delete if appropriate)
Do you give consent for us to contact other professionals who are involved with your child?	Yes/No (Please delete if appropriate)
Names and contact numbers of any professionals involved with your child, for example health visitors, speech therapists. If you provide these details we will contact them, letting you know of any approach we make.	
Please give details of any other problems/concerns of which the school should be aware to enable us to support your child. If you provide these details we will contact them, letting you know of any approach we make.	
Please give details of any special requirements/medical conditions of parents/carers regarding access to the building or accessing information	

School Trips & Off Site Visits

Please review your policies in respect of school trips. Acceptance of the risks, insurance issues and all other issues are subject to individual policies. This clause needs to be inserted.

'When making arrangements for school trips it is necessary to share information about your child with the venue, accommodation and transport providers for legal and safeguarding reasons. If travelling overseas this will also include immigration control.

Details about your child may be required by insurers.'

FOR TRIPS OUTSIDE THE UK

'Whilst pupils are outside the UK school staff and those supervising, travelling or arranging travel or accommodation may communicate with parents and carers using the contact information provided. At times this may be using mobile communications, social media or other methods that may require data to be stored or travel outside of the approved EU locations. We believe that keeping parents and carers informed about the wellbeing of their children must be the priority. Data sharing in such cases will be limited to what is necessary.'

	Y	N

I give consent for school to take photographs of my son/daughter whilst on school trips.		
I give consent to school/college to take video and media footage of my son/daughter whilst on school trips		

Careers & Workplace Placements

	Y	N
I give consent for school/college to share details of my son/daughter with potential workplace placement providers		
I give consent to school/college to share details of my son/daughter with careers advisers		

School Work & Celebrating Successes

	Y	N
I give consent for school to share details of my son/daughter's achievements within school by displays, certificates or other media that identifies them		
I give consent to school/college to share information about my son/daughter to recognise key events such as birthdays within the school community		
I give consent for school/college to share details of my son/daughter's sporting activities for fixtures and achievements in school and in publications		

Internet Use

As part of the school's IT provision we offer students access to the internet and email facilities. Our internet service provides a high level of protection and we audit student use. Students are required to give written agreement to be bound by the terms.

	Y	**N**
As the parent or carer, I give permission for my child to use electronic mail and the internet. I understand that students are held accountable for their own actions.		

Childcare Costs, FSM and PP

https://www.childcarechoices.gov.uk/

Parents and carers must be informed that they can check themselves.

	Y	**N**
I give consent for school/nursery to use my details, including National Insurance number, to check eligibility for Child Care place funding, Free School Meals and/or Pupil Premium		

I consent to the school/nursery to retain this information on file to continue to monitor eligibility		

School News Updates

	Y	N
I wish to be kept informed about school news and events and receive the newsletter and similar notifications		
I consent to the school to use text messaging service on the mobile number I have provided.		
I consent to the school contacting me by text message for the purpose of school information and reminders. I will ensure that I keep the school informed of my up to date mobile number at all times, or if the number is no longer in my possession		

(PLEASE NOTE: WE CANNOT ACCEPT INCOMING TEXT MESSAGES.)

Biometrics

YOU MUST PROVIDE DETAILS OF THE SCHEME ALSO AS ADDITIONAL INFORMATION

	Y	N
I give consent to information from the finger scan of my child (named above) being taken and used as part of an automated biometric recognition system for access to cashless dining facilities, library and in school ICT services. I understand that I can withdraw this consent at any time in writing.		

Third Parties at School

IF YOU CHOOSE TO INCLDUE THESE MAKE IT CLEAR THAT UNLESS CONSENT IS GIVEN THE CHILD CANNOT PARTICIPATE

	Y	**N**
I give consent for school to share details with organisers of end of school events, such as discos and concerts. This is to enable children to be checked in and out of the event securely.		
I give consent to the school to share basic details with third party providers, such as before and after school clubs, music and sport providers who may be engaged directly by me.		
I give consent to the school that they can share information about my son/daughter with organisations such as the Duke of Edinburgh scheme		

Subject Access Request – Requester Overview

As an organisation we collect and process data about individuals. We explain what information we collect, and why in our Privacy Notices.

Any individual, or person with parental responsibility, or young person with sufficient capacity to make a request is entitled to ask what information is held. So that person is the 'Requester'.

Copies of the information may also be made available on request. A form to complete is available.

To ensure that requests are dealt with in an effective and timely manner we may seek to clarify the terms of a request.

To collate and manage requests each school will have an individual allocated to co-ordinate all requests. **That information is available on the school website and the Subject Access Request form.**

What happens next?

There is a SAR request form on the website. We encourage everyone to use this form as it enables us to make sure you are being provided with the actual information that you require.

Please complete the for, and provide the necessary information, and send it back to the school.

Evidence of the requester's identity may be required. Discretion about employees and person known to the school may be applicable but if ID evidence is not required an explanation must be provided by school staff and signed and dated accordingly.

We may need to contact you to clarify details about what you have requested.

We may need to contact other people and 3rd parties, who have provided information that is on our files.

Providing the Information

We need to review the information to see what can be shared, or if any item needs another person's consent. It may be that some information is subject to an exemption and cannot be shared.

Exemptions to a SAR exist and may include:

- Education, Health, Social Work records
- Examination marks and scripts
- Safeguarding records
- Special educational needs
- Parental records and reports
- Legal advice and proceedings
- Adoption and Court records and/or reports
- Regulatory activity and official requests e.g. DfE statistical information
- National security, Crime and taxation
- Journalism, literature and art
- Research history, and statistics

- Confidential references

All data subjects have the right to know:-

- What information is held?
- Who holds it?
- Why is it held?
- What is the retention periods?
- That each data subject has rights. Consent can be withdrawn at any time (to some things).
- A right to request rectification, erasure or to limit or stop processing
- A right to complain

Much of this will be contained within the Privacy Notices and other information on our website.

Provision and Timeline

The information will be provided in an electronic format, usually within one calendar month of the request. However in some circumstances, if the request is complex or it is difficult to access the information, this may be extended by up to another 2 calendar months.

Information is usually provided in a secure electronic format.

Following delivery of the information the requester has the right to ask for a review or use the complaint process if they feel that information has not been pro

Information Sharing Principles

Information sharing occurs on a daily basis in schools. It may be information about pupils, staff, parents or others. Every member of school staff, and many volunteers, have access to a lot of information about different individuals.

For all of us, we have to bear in mind the basis that we share and discuss information. UK GDPR and Data Protection is only part of the story. Safeguarding, contractual responsibilities, statutory responsibilities and daily expectations are all other factors why we share information.

Schools have many policies that deal with all aspects of school life. Every member of a school staff needs to consider some key elements when they are sharing information.

The purpose of sharing

Sharing information can be as simple as the word of a parent in the playground, by email or by telephone. It may be something as simple as "yes Tom had a good day" or "Kirpal enjoyed the music lesson". It might be far more intricate and complicated. It could be information about a child's injury at school. A health issue. Concern about behaviour, bullying or SEN. All of these are examples of information sharing.

Who are we sharing with?

Who is the recipient of the information? Do they have a legitimate right to know the information? Is it a parent or someone with Parental Responsibility? Is it an external partner agency like the police or social care? Is it an extended family member? Or even a sibling?

Thinking about who the recipient is, and what is their legal basis for requesting the information, needs to be at the forefront of all school staff's consideration.

What data is to be shared?

Some information is more sensitive, and sharing health information or safeguarding information must be done with great care. However, even some basic information about pupils or staff needs to be thought through carefully. When you are asked to share information, you need to consider what is the least amount of information that can be shared to fulfil the objective. Data minimisation is a key pillar of the UK GDPR – keep it as brief as possible.

Data quality, accuracy, relevance and usability

What information is being given? Is it an opinion or is it fact? If it is reporting information that is not known directly by you, what is the source of it? Are you sure it is accurate? Are you providing information that was given to school for one reason, but the requester wants it for a different purpose? If so, is it right to share that information?

Data security

How is the information to be shared? Face-to-face, is it a safe place to have a confidential conversation? Are are other people around? Should confidential information be sent by email? What about secure delivery, or password protection? If being shared with an outside agency, what protections are in place? If information is going out by hard copy post, what checks and balances are there to make sure that the right recipients get the right report? (This is a common source of a data breach).

If information is going by pupil post, are there any risks if the bag went missing on the way home?

Are there measures in school to ensure that information is checked on an annual basis and reminders are sent through the academic year for parents and carers to update contact information?

Record-keeping

It will be impossible to keep track of every piece of information that is shared in the school. A school would grind to a halt within half an hour! However, sensitive information or safeguarding or health data being shared should be recorded. This might be as simple as keeping a note on an email about what was sent and why.

Individual's rights

All staff members should be aware that there are Data Subject Access processes that individuals can use. Likewise, there is a complaints process that can be accessed and people should be directed to the relevant pages on the school website or in the policies.

SAR request form

Data Subject (person who information is about)

Title	
Name	
Date of Birth	
Year group (if child or young person)	

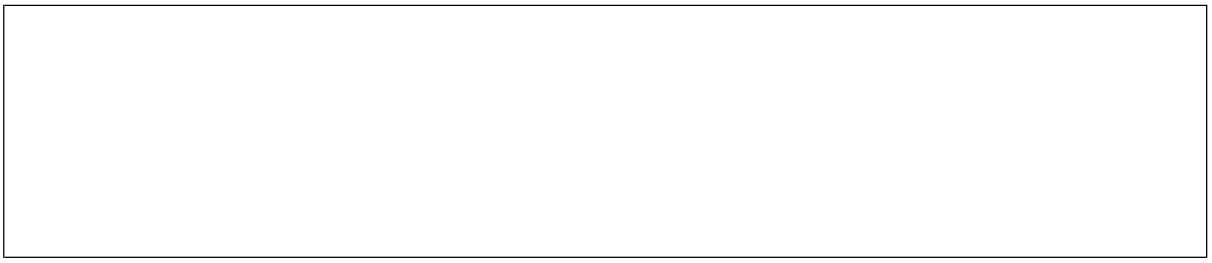
Person making the request

Name	
Date of Birth	
Address	
Email Address	
Contact phone no	
Identification Evidence Provided (if required) Passport Driving licence Or two forms of Utility bill within last 3 months Bank statement of last three months Council Tax bill Rent book	

Status of person making request

Parent or person with Parental Responsibility	
Are you acting on their written authority (please provide a copy of the consent)	
If not the parent or with PR, what is your role?	

Details of Data Requested



Declaration

I, ……., hereby request that XXXXX provide the data requested about me.

Signature: Dated:

I, ……., hereby request that XXXXX provide the data requested about
……..(insert child's name) on the basis of the authority that I have provided.

Signature: Dated:

Freedom of Information Policy

Cavendish Close Infant School is subject to the Freedom of Information Act 2000 (FOI) as a public authority, and as such, must comply with any requests for information in accordance with the principles laid out in the Act.

This means that the school must hold and publish a FOI Publication Scheme, to communicate what information we hold is readily available to the public, and where it can be found.

All public authorities must also have processes in place to manage any FOI requests that are made.

Freedom of Information Publication Scheme

The School publication scheme has been developed from the Information Commissioner's Office template documents. It is the trust's aim to ensure that the publication of information is accessible for individuals. Much of the information listed is routinely published on individual school websites and in their individual prospectuses.

The publication scheme and the material it covers will be readily available in hard copy from the trust or the individual school, depending on the source of the information.

Where the cost of postage, printing or photocopying is below £10.00, we will not make a charge.

Where it is over £10.00, the first £10.00 will be free of charge, after that we will charge the full estimated cost of postage and copying.

Before we produce the information, we shall inform you of the total cost. You may wish to refine the request in order to reduce the cost and we would be happy to discuss this with you.

Freedom of Information requests

Any request for any information from the trust or our individual schools will be considered to see if it meets the criteria of FOI. This is irrespective of whether or not the individual making the request mentions the FOI.

If the request is simple and the information is to be released, then the individual who received the request can release the information, but must ensure that this is done within the timescale set out below.

A copy of the request and response should then be sent to the School Business Manager.

All other requests should be referred in the first instance to the officer who may co-ordinate the process with other staff.

All requests under FOI are treated as if made by any member of the general public. Any information released will be within the public domain and may not be marked restricted or confidential.

Time limits for FOI requests

The trust and/or school must respond as soon as possible, and in any event, within 20 working days of the date of receipt of the request. When calculating the 20 working day deadline, a “working day” is a school day (one in which pupils are in attendance), subject to an absolute maximum of 60 normal working days (not school days) to respond.

Procedure for dealing with a request

All FOI requests should be forwarded on receipt to the specified co-ordinator in each school.

Initially it will be necessary to determine whether or not the organisation holds the information requested. This might be in hard copy or digital media.

There may be occasions where information is held, but the process of extracting the relevant information would take considerable time. In those instances the requester may be given the opportunity to refine the request based on the information given.

Part 1 – Identifying the types of information

As an organisation we hold different types of information.

Organisational information, prospectus, locations and contacts, constitutional and legal governance, schemes of delegation, individual school arrangements.

Financial information about income and expenditure, financial audit, funding agreements, procurement, tendering and contracts.

Plans, strategies, aims and objectives, performance indicators, audits, inspections and reviews.

Decision making processes and records of decisions, internal criteria and procedures

Policies and procedures –protocols, policies and procedures for delivering services and compliance with our statutory and regulatory obligations.

Lists and registers required by law and other key information.

Details of our curriculum and wider educational offering

Part 2 - Considering the nature of the request

FOI requests will be fully complied with unless an exemption applies.

Common exemptions in the Freedom of Information Act 2000 include:

Section 40 (1) – the request is for the applicants personal data. This must be dealt with under the subject access regime in the GDPR, see the Data Protection Policy and Privacy Notices;

Section 40 (2) – compliance with the request would involve releasing third party personal data, and this would be in breach of the GDPR principles as set out in Data Protection Policy

Section 41 – information that has been sent to the Academy Trust (but not the Academy's own information) which is confidential;

Section 21 – information that is already publicly available, even if payment of a fee is required to access that information;

Section 22 – information that the Academy Trust intends to publish at a future date;

Section 43 – information that would prejudice the commercial interests of the Academy and / or a third party;

Section 38 – information that could prejudice the physical health, mental health or safety of an individual (this may apply particularly to safeguarding information);

Section 31 – information which may prejudice the effective detection and prevention of crime – such as the location of CCTV cameras;

Section 36 – information which, in the opinion of the chair of trustees of the Academy Trust, would prejudice the effective conduct of the Academy. There is a special form for this on the ICO's website to assist with the obtaining of the chair's opinion.

Information within these exemptions must be considered and weighed up about the general principal that information should be disclosed wherever applicable.

Part 3 - Responding to a request

When responding to a request where it is necessary to withhold some or all of the information, we will explain why the information has been withheld, quoting the appropriate section number and explaining how the information requested fits within that exemption. If the public interest test has been applied, this will be set out.

In these circumstances the requester can seek a review form with the trust school, and correspondence should be addressed in the first instance to the CEO? Head? School Business Manager.

If anyone has any concerns, questions or complaints in relation to this policy or the publication scheme contained within it they should contact XXXXXXXXXXXXXXXXX trust or school details to add

If you require a paper version of any information set out under the FOI Publication Scheme, or want to ask whether information is available, contact the trust using the details set out below.

Contact

As outlined above, please contact XXXX for any FOI requests.

You can also visit our website www.trust/school.co.org.uk. To help us process requests quickly, any correspondence should be clearly marked 'FOI Request'.

If you are not satisfied with the assistance that you get or if we have not been able to resolve your complaint and you feel that a formal complaint needs to be made then this should be addressed to: Information Commissioners Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5A, telephone: 0303 123 1113, website: www.ico.org.uk

Safe and Acceptable Use / Bring Your Own Device Considerations - Staff

Cavendish Close Infant School recognise that many staff choose to access school information from their own devices.

Any member of staff wishing to do this must be aware that they have a direct personal responsibility for ensuring that the device they choose to use has the benefit of encryption, that is above and beyond a simple password protection.

Staff must ensure that personal devices such as mobile smart phones, tablets and other portable electronic equipment are set to lock and only open with encrypted passcodes to prevent unauthorised access.
School can provide support if requested, and enable staff to ensure that their devices are compliant.

If any member of staff uses a device without these safeguards in place it will be a disciplinary breach if data is unlawfully accessed by a third party.

Encryption protection will be available for staff and suitable advice provided.

Own Device Usage Acceptance

I, ……., understand and accept that should I choose to access school data on any personal device that I use or own must have, and use, suitable encryption to secure the data. Any unlawful access of data on such a device will be my responsibility. I will report any theft or loss to the school compliance manager/SBM/DPO as soon as is practicable.

When exchanging, gifting, upgrading or selling the device, I shall ensure that access to any school data is removed and data that relates to school is securely deleted.

Mobile phones are to be off or on silent, and out of sight and reach of children, in a high/locked cupboard

Smart watches are not to be accessed during learning time, or to be near the children.

Name	Signed	Date

Cavendish Close Infant School the Publication Scheme

This is a list of information we hold. Not all will be released as part of an FoI request. All requests will be considered in line with our policy and obligations.

Information available	How the information can be obtained	Charge
Information, structure, locations and contacts Current information only		
Who's who in Cavendish Close Infant School	Website	No charge
Governing body – names and contact details of the governors and the basis of their appointment	Individual School websites	No charge
Instrument of Government –Funding Agreements	DfE website	No charge
Staffing structure	Trust & Individual School Websites	No charge
School Session times, term dates and holidays	Trust & Individual School Websites	No charge
Location & Contact information – address, telephone numbers & website	Trust & Individual School Websites	No charge
Contact details for the Principal and the Governing Body	Trust & Individual School Websites	No charge
School Prospectus	Individual School Websites	No charge

Information available	How the information can be obtained	Charge
Financial information relating to projected and actual income and expenditure, procurement, contracts and financial audit (Minimum of current and the previous two years financial year)		
Annual financial statements, capital funding and income generation for prior years	Hard copy and on website	No charge

Details of capital funding allocated to the school along with information on related building projects and other capital projects or sources of funding for current year	Electronic copy through request to admin@cavclosei.derby.sch.uk	No charge

Procurement and contracts, subject to the commercial/confidential public interest test	Electronic copy through request to admin@cavclosei.derby.sch.uk	No charge
Pay Policy – statement on general procedures	Hard copy	Schedule of charges
Staff grading and structure	Hard copy	Schedule of charges
Governors' allowances – details if allowances/expenses that can be claimed/incurred	Hard copy	Schedule of charges

Information available	How the information can be obtained	Charge
Strategies and plans, performance indicators, audits, inspections and reviews Current information as a minimum		
School Profile -Government supplied data -Latest OFSTED report – summary and full report -Examination results	DfE Website Ofsted website School website School website	Schedule of charges No charge No charge
Performance Management policy and procedures	Hard copy	Schedule of charges

Future plans	Trust & Individual School Websites	No charge
Safeguarding policies and procedures	Hard copy & School Website	Schedule of charges

Information available	How the information can be obtained	Charge
Decision making processes and records of decisions Current and previous three years as a minimum		
Admissions policy and decisions (not individual decisions)	Individual school websites	No charge
Governing Board meeting agendas and minutes – (this will exclude information that is properly regarded as confidential to the meeting)	Hard copy	Schedule of charges No charge

Information available	How the information can be obtained	Charge
Current written protocols, policies and procedures for delivery our services and responsibilities Current information as a minimum		

Policies including: Charging and remission policy Health & Safety and Risk Assessment Complaints procedure Staff, discipline, grievance, pay and conduct Policies Staffing structure implementation plan Equal Opportunities policies – including equality & diversities Staff Recruitment & Selection policies Child Protection Policy	Hard copy School websites	No charge

Pupil and curriculum policies including: Relationships and Health Education Policy Special Needs Educational Policy/Information Report Accessibility Policy	Hard copy & Individual school websites	No charge

Information available	How the information can be obtained	Charge
Procedures and Policies Current information as a minimum		

Pupil and curriculum policies including: (cont'd) Pupil Behaviour, Discipline Exclusion Policy Equality Information & Objectives	Hard copy & Individual school websites	No charge
Records Management and Personal Data Policies: Information security policies Records retention policies Destruction and archive policies Data Protection policies	Hard copy	No charge
Charging Regimes and policies: includes details of any statutory charging regimes – charges made for information routinely published. Clearly stating what costs are to be recovered, the basis on which they are made and how they are calculated.	Hard copy	No charge

Information available	How the information can be obtained	Charge
Lists and Registers only		
Curriculum circulars and statutory instruments	Hard copy	Schedule of charges
Disclosure Logs	In school	Schedule of charges
Asset Register	In school	Schedule of charges
Any information the Trust are currently legally required to hold in publicly available registers	Hard copy	Schedule of charges
Information services Currently information only		
Extra-curricular activities Out of School Clubs	Individual School websites	No charge
School publications	Individual School websites	No charge
Services for which the school is entitled to recover a fee, together with those fees	Individual School websites	No charge
Leaflets, booklets and newsletters	Individual School websites	No charge