

Data Protection Policy



Mission Statement

We will all work to be Outstanding delivering opportunities for successful learning. Our school will be a safe, happy place that allows everyone to reach their best or beyond! We will work to coach each other in order to provide an excellent, enriched and enhanced curriculum that inspires progress. Our learning culture for all will be felt at all times. We are all in this together.

Date of Policy	May 2018
To be reviewed	May 2019

What is the GDPR?

This is a European Directive that was brought into UK law with an updated Data Protection Act for May 2018. Brexit will not change it.

The previous Data Protection Act 1998 has been repealed and replaced with the Data Protection Act 2018.

What is the point of the GDPR?

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

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

Who does it apply to?

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

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 identified 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.

Every school also has to publish a Privacy / Fair Processing Notice on the website.

What are the key principles of the GDPR?

Lawfulness, transparency and fairness.

School must have a legitimate reason to hold the data, we explain this in the Data Privacy Notices on the website. 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 sometimes when you cannot withdraw consent as explained in 'Data Subjects Rights'.

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

So, 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. We do this when pupils join the school and check on an annual basis.

If a Data Subject feels that the information held is inaccurate, should not 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.

Retention

Carlyle Infant and Nursery School has a retention policy that explains how long we store records for. This is available on request from our school office. Details are displayed on the school website.

Security

We have processes in place to keep data safe. That might be paper files, electronic records or other information. We ensure that data held on paper or electronically is stored in a secure location (locked filing cabinet, office or encrypted files), usable by only those deemed suitable to use.

Who is a 'data subject' ?

Someone whose details we keep on file. Some details are more sensitive than others. The 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, 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.

Subject Access Requests

You can ask for copies of information that we hold about you or a pupil who you have parental responsibility for or are a parent of at school. 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, for example, the school was closed for holidays. The maximum extension is up to two months.

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 in an 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'?

Our school governing body is the data controller. They have ultimate responsibility for how school manages data. They delegate this to data processors to act on their behalf.

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 LA.

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

Processing data

We must have a reason to process the data about an individual. Our privacy notices set out how we use data. The 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 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 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.

(The Breach & Non Compliance Procedures and Policy document can be located in the appendix.)

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. However, in most cases data will only be processed if explicit consent has been obtained.

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.

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.

We review the contact and consent form on an annual basis. It is important to inform school if details or your decision about consent changes. A form is available.

Pupil Consent Procedure

Where processing relates to a child under 16 years old, school will obtain the consent from a person who has parental responsibility for the child.

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 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:-

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

Our DPO is John Walker, Solicitor for Flint Bishop. Details can be obtained from the school office.

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 Site Manager is responsible for authorising access to secure areas along with SLT.

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

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 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, 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 GDPR compliance and processes will be conducted by the Data Protection Officer biannually.

Appendix 1

Acceptable Use / Bring Your Own Device Considerations - Staff

Carlyle Infant and Nursery 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 will support 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, INSERT NAME, 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 Business Manager and this will then be reported to our 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.

Name	Signed	Date

Appendix 2

Information Access Request Record

Pupil / Individual Name	
DoB	
Date info requested	
Who was the requester?	
How were they positively identified?	
What information was requested?	
Basis for the request?	
Was information disclosed? Yes No	
Reason for decision	
What was disclosed?	
If CP or Criminal concern is this whole record confidential? Give reasons and make clear on system	
Authorisation by	
Date	
Staff member(s)	

Appendix 3

GDPR and Data Protection Training and Awareness Protocol

Carlyle Infant and Nursery School want to ensure that staff and school volunteers have access to appropriate resources to enable compliance with GDPR and data protection principles.

Obligations to secure suitable CPD for school staff and governors will be a consideration when determining the necessary level of training for each role.

The Data Controller is responsible for the identification and delivery of suitable training and deployment of suitable resources. Personnel will need to feel confident in understanding how GDPR applies to their own role and the school and organisation overall.

The training and CPD must ensure that school personnel are aware of day-to-day obligations to manage personal data and process it with due respect. Those with regular access to personal data, to manage and update systems and to use the data must demonstrate and understand the requirement to be compliant with the GDPR.

The Data Protection Officer/Data Protection Compliance Manager shall ensure regular updates will be provided to continue to raise awareness. Training needs will be considered as part of performance management and strategic development for the whole school community.

We shall provide staff with specific training on processing personal data relevant to their individual day-to-day roles and responsibilities, and in accordance with our policies and procedures. This identifies key areas of data protection and security issues that are relevant to role and responsibility.

The HR lead shall retain records of the relevant training and CPD undertaken by each person. A clear process for recording training and CPD will be in place for all relevant personnel. This will be for employed staff and volunteers.

Appendix 4

Non Compliance Protocol

It is important that any non compliance is brought to the attention of the **Data Protection Compliance Manager / Data Protection Officer** to enable an action plan to be developed and implemented. This record will also serve as a useful mechanism to identify trends, risks and potential breach hazards.

By having an agreed timescale for review, identifying training needs that may be applicable to an individual or group of people will assist future compliance.

Appendix 5

Retention Policy Overview

A comprehensive retention policy is in place. It is available on request/on the website

The Data Controller must ensure that a suitable retention policy is in place and is effective.

This will be with the support of the DPO/Data Compliance Manager. Procedures to manage disposal and retrieval of stored data, such as encryption keys and passwords, must also be set out within the retention policy.

Within Carlyle Infant and Nursery School responsibility for secure retention and review is as follows

Type of Data	Responsible Person
Pupil Progress and Attainment	
SIMS or equivalent	
Financial	
Human Resources	
Health and Safety Records	
Governance	
Hardware	
Software	
Statutory and Regulatory	
SEN and Health	
Safeguarding	
Servers	
IT to include PCs, laptops and portable storage	
Digital records	
Emails	

Access Control Rules and Rights for Users guidance sets out the level of access across the organisation.

Destruction

At the point of destruction the 'Data Destruction Log' will be completed

Appendix 6



Consent Withdrawal Form – Individual

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 (Carlyle Infant and Nursery 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:

Appendix 7

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

(Carlyle Infant and Nursery 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:

Appendix 8

Third parties and the Data Controller

The Data Controller is responsible for ensuring that correct protocols and agreements are in place to ensure that personal data is processed by all sub contractors and other third parties in line with the principles of the GDPR.

Individuals within school who have a responsibility for securing contracts and agreements with such third parties are responsible for ensuring that all external data processing is contracted out in line with the GDPR principles. This will include:-

IT contracts and processes

Physical data and hard copy documents

Data destruction and hardware renewal and recycling

Financial and personnel information

Pupil and staff records

Only suppliers that can confirm they have appropriate technical, physical and organisational security to securely process data will be considered as suitable partners.

The procurement process will ensure that all contracts are suitable and reflect GDPR requirements. Review of current and due consideration of future contracts will require this even if data processing is ancillary to the main purpose of the contract.

The external processor will confirm with the data controller that suitable security and operational measures are in place.

Any potential supplier or purchaser outside the EU will be obliged to confirm how they comply with the GDPR and give contractual assurances.

The DPO/SBM/Data Protection Compliance Manager may require a specific risk assessment to be undertaken if the data is sensitive and if an increased risk is likely due to the nature, or proposed nature, of the processing.

A written agreement will be in place between the supplier and the school to confirm compliance with the GDPR principles and obligations to assist the school in the event of data breach or subject access request, or enquiries from the ICO.

The school must have the right to conduct audits or have information about audits that have taken place in respect of the relevant processes of the supplier's security arrangements whilst the contract is in place, or whilst the supplier continues to have personal data that relates to the contract on its systems.

Any subcontracting must only be done with the written consent of the school as data controller. This must be the case for any further subcontracting down the chain. All subcontractors must confirm agreement to be bound by GDPR principles when handling the school's data, which shall also include co-operation and eventual secure destruction or return of data.

Appendix 9

Data Protection Breach & Non Compliance Procedure

All staff, governors and trustees must be aware of what to do in the event of a DPA / 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.

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.

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

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.

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.

Date	Evidence Description	Secure storage location & confirmed date	School Officer

Data Breach Notification Form

When did the breach occur (or become known)?	
Who was involved in the school?	
Who was this reported to?	
Date and time it was reported	
Date and time DPO notified	
A description of the nature of the breach. This must include the type of information that was lost, e.g. name, address, medical information, NI numbers	
The categories of personal data affected – electronic, hard copy	
Approximate number of data subjects affected.	
Approximate number of personal data records affected.	
Name and contact details of the Data Protection Officer / GDPR Owner.	
Consequences of the breach. What are the potential risks?	
Any measures taken to address the breach. What actions and timeline have been identified?	
Any information relating to the data breach.	

Appendix 10

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.

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. The data subject(s) will be notified of the right to complain directly to the Information Commissioner, whose details will be in the response.

Appendix 11

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 Carlyle Infant and Nursery School provide the data requested about me.

Signature:

Dated:

I,, hereby request that Carlyle Infant and Nursery School provide the data requested about

.....(insert child's name) on the basis of the authority that I have provided.

Signature:

Dated:

Appendix 12

Subject Access Request – Process and Protocol

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. Copies of the information shall 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 we have designated **XXXXX** to co-ordinate all requests. Please ensure that requests are made on the form to **XXXXX**.

Evidence of their identity, on the basis of the information set out and the signature on the identity must be cross-checked to that on the application form. Discretion about employees and persons 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

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

Many of these questions will be within the Privacy Notices on the website.

The information will be provided in an electronic format, usually within one calendar month of the request. However in some circumstances, for example the school is closed for holidays, this may be extended by up to another calendar month.

Appendix 13

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.

Appendix 14

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 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 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

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 school employees with our local authority (LA) and the Department for Education (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Data collection requirements

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

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

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

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

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

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

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

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

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

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact our School Business Manager.

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 policies for the School Workforce on the website.

Appendix 15

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 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 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 O'Track 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 will be investigating using systems to take electronic payments. 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/>

Contact:

If you would like to discuss anything in this privacy notice, please contact the school office for the School Business Manager.

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.

