



GENERAL DATA PROTECTION REGULATIONS (GDPR) POLICY

Data Protection Controller – Every Child Matters Academy Trust
Data Protection Officer – Deb Barker

Legal framework

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

- The General Data Protection Regulation (GDPR)
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998

This policy will also have regard to the following guidance:

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'

Introduction

Every Child Matters Academy Trust (The Trust) collects and uses personal information about staff, pupils, parents and other individuals who come into contact with schools in the Trust. This information is gathered in order to enable its' schools to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the Trust and its' school comply with their statutory responsibilities. This policy applies to all data, regardless of whether it is in paper or electronic format.

Trusts have a duty to register as a Data Controller with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are available on the ICO's website.

Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 1998 (DPA), and other related

legislation including the GDPR. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be made aware of their duties and responsibilities and adhering to the guidelines set out in this policy.

What is Personal Data?

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held. This person is referred to as a "Data Subject". To qualify as personal data, the data must allow you to identify and give information relating to a data subject. Personal data includes facts and any expression of opinion about an individual.

Examples of personal data are: names and addresses; bank details; academic, disciplinary, admissions and attendance records; references; and examination scripts and marks.

Sensitive personal data is defined in the GDPR as information in respect of racial or ethnic origin, political opinions, religious beliefs or "other beliefs of a similar nature", membership of a trade union, physical or mental health, sexual life, criminal convictions and alleged offences. Sensitive personal data can only be processed under strict conditions, including a condition requiring consent of the person concerned to such processing.

Processing Personal Data

Processing of personal data includes obtaining, holding, recording, adding, deleting, augmenting, disclosing, destroying, printing or otherwise using data. Processing also includes transferring data to 3rd parties.

Consent may be required for the processing of personal data unless the processing is necessary for the school to undertake their obligations to pupils and their parents or guardians. Personal data, unless otherwise exempt from restrictions on processing under the DPA, will only be disclosed to third parties under the terms of this policy or otherwise with the consent of the appropriate individual.

The rights in relation to personal data set out under the DPA are those of the individual to whom the data relates. The school will, in most cases, rely on parental or guardian consent to process data relating to pupils, and those with 'parental responsibility' are entitled to receive relevant information concerning the child.

GDPR Principles

- processed lawfully, fairly and in a transparent manner in relation to individuals (*addition of transparency*)
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (*widens the scope of further processing by controllers for such things as scientific purposes etc.*)

- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (*DPA says not excessive where GDPR now specifies processing be limited to only necessary*)
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (*largely the same, though expressly states “every reasonable step” be taken to ensure accuracy*)
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals (*largely the same but expands on the list of exemptions*)
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (*GDPR mirrors the values within the DPA*)

The Trust and all staff or others who process or use personal information must ensure that they follow these principles at all times.

Lawful Processing

The legal basis for processing data will be identified and documented prior to data being processed.

Under the GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained.
- Processing is necessary for:
 - Compliance with a legal obligation.
 - The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
 - For the performance of a contract with the data subject or to take steps to enter into a contract.
 - Protecting the vital interests of a data subject or another person.
 - For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (This condition is not available to processing undertaken by the school in the performance of its tasks.)

Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.

- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for:
 - Carrying out obligations under employment, social security or social protection law, or a collective agreement.
 - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
 - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
 - Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards.
 - The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.
 - Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
 - Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.

— Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.

— Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

7. Consent

7.1. Consent must be a positive

Responsibilities

The Board of Trustees has overall responsibility for compliance with the DPA. At each school in The Trust, the Headteacher is responsible for ensuring compliance with the DPA and this policy.

All members of staff or contractors who hold or collect personal data are also responsible for their own compliance with the DPA and must ensure that personal information is kept and processed in-line with the DPA.

All staff must as a minimum check that any personal data that they provide to the Trust in connection with their employment is accurate and up to date. They must also inform the Trust of any changes in their personal data that they have provided, e.g. change of address, either at the time of appointment or subsequently.

Staff should report any unauthorised disclosure, loss of personal data, or other breach of this policy immediately to the Data Protection Officer, in order to minimize potential damage to data subjects, or to the reputation of the school/trust. Failure to report a data breach will be treated a disciplinary matter, and may be considered gross misconduct in some cases. All breaches will be investigated by the Data Protection Officer and reported to the I.C.O. if deemed necessary who have the power to levy fines dependant on the severity of the data breach.

The Trust will take appropriate organisation and technical measures to ensure that any third parties who process personal data on behalf of schools in the Trust, do so in a manner that permits the Trust to uphold its statutory responsibilities in relation to data protection.

All staff will receive training on processing personal data, through our induction and as part of our staff development programme.

Fair Processing/ Sharing Personal Data

All schools in the Trust have a duty to issue a Privacy Notice to all pupils/parents and staff, this summarises the personal data we hold, why it is held and the other parties to whom it may be passed on to or with whom it may be shared.

Parents/Carers will be issued with a copy of our Privacy Notice (Appendix A) for pupils at the beginning of each academic year. A copy of this notice will also be available on the relevant school website.

Staff will be issued with a copy of our Privacy Notice (Appendix B) for the school workforce on induction and a copy of this notice will also be available in the Staff Handbook/Induction Pack.

If we need to share personal data with third parties, we will not do so unless:

- the data subjects have given their consent;
- to safeguard national security;
- for the prevention or detection of crime;
- to prevent serious harm to the data subject or a third party;
- for the assessment of any tax or duty;
- where it is necessary to exercise a right or obligation conferred or imposed by law upon the school (other than an obligation imposed by contract);
- for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings); and
- for the purpose of obtaining legal advice;

It is a criminal offence to knowingly or recklessly obtain, or share (disclose) information about an individual without legitimate cause. Relevant, confidential data should only be given to:

- other members of staff on a need to know basis;
- relevant Parents/Guardians;
- other authorities if it is necessary in the public interest, e.g. prevention of crime;
- other bodies, such as the Local Authority and schools to which a pupil may move, where there are legitimate requirements.

The Trust and its schools will not disclose any information from a pupil's record which would be likely to cause serious harm to their physical or mental health or that of anyone else.

Where there is any doubt, or statutory requirements conflict we will seek additional advice before disclosing personal information.

When giving information to an individual, particularly by telephone, it is most important that the individual's identity is verified. So, from time to time we may need to ask parents/carers additional questions, to which only he/she is likely to know the answers. Information will not be provided to other parties, even if related. For example: in the case of divorced parents it is important that information regarding one party is not given to the other party to which he/she is not entitled.

Where we are required to share personal data with other agencies, this will be done through secure transfer mechanisms.

Any person whose details are held by a school in the Trust is entitled, under the provisions of the DPA, to ask for a copy of all information held about them (or child for which they are responsible). Please see Appendix C, D and E for details on how our Trust deals with Subject Access Requests.

Disclosure of personal data to third parties

The school may receive requests from third parties (i.e. those other than the data subject, the school, and employees of the school) to disclose personal data it holds about pupils, their parents or guardians. This information will not generally be disclosed unless one of the specific exemptions under the DPA which allow disclosure applies; or where necessary for the legitimate interests of the individual concerned or the school.

The following are the most usual reasons that the school may have for passing personal data to third parties. To:

- publish the results of public examinations or other achievements of pupils of the school;
- disclose details of a pupil's medical condition where it is in the pupil's interests to do so, for example for medical advice, insurance purposes or to organisers of school trips;
- provide information to another educational establishment to which a pupil is transferring;
- provide information to the Examination Authority as part of the examinations process; and
- provide the relevant information to the Government Department e.g. Department for Education, Ofsted, concerned with national education.

The DFE uses information about pupils for statistical purposes, to evaluate and develop education policy and to monitor the performance of the nation's education service as a whole. The statistics are used in such a way that individual pupils cannot be identified from them.

Any wish to limit or object to any use of personal data by third parties, except as stated above, and should be notified to the Data Protection Officer of the relevant school in writing.

Where the school receives a disclosure request from a third party it will take reasonable steps to verify the identity of that third party before making any disclosure. When members of staff receive enquiries from third parties for personal data, the enquirer should be asked why the information is required. If consent to the disclosure has not been given (and an exception does not apply) then the request should be declined. In normal circumstances information should not be disclosed over the phone to third parties. In most circumstances third parties should be asked to provide documentary evidence to support data requests.

Data Sharing Agreements with Third Party Organisations

Schools within the Trust have third party agencies offering guidance and support services to pupils on a 1:1 basis. Examples of such services include the Educational Psychology Service SALT, and various 'counselling' services. If such services operate on our school site, there are Data Protection and Confidentiality issues to consider.

In normal circumstances many services of this type offer a confidential service to pupils and will only share data with the school or parents with the consent of the pupil (age 12+) or in cases where an over-riding Duty of Care exists (e.g. if the pupil or someone else is in danger).

When such services are delivered on school premises, the school has the right to agree to the confidential nature of such a service or, alternatively, the school may insist that the service operates within the school policy on data handling. This latter approach places an expectation on the service to automatically keep the school informed of the content of sessions, held at the school, involving pupils.

It is good practice to agree the approach to confidentiality from the outset to avoid incorrect assumptions being made by either party.

- In the Service Level Agreement (SLA) with the agency, the school's expectation on confidentiality should be clearly stated. The SLA should require agency staff to make pupils/parents aware of the confidential nature, or otherwise, of the service.

A template agreement document between a school and third party agency is attached which may be appended to SLA documents. There are two examples depending on whether the School is happy for a confidential service to take place or not. See Appendix G and H.

Information Security

The Trust is committed to take the necessary precautions to protect the security of personal data it is responsible for.

Access to school sites is restricted and the personal data of pupils is not visible via the public areas of school receptions.

The Trust has taken appropriate security measures to protect personal data stored within school buildings from theft, damage or other unauthorised disclosure.

Inside school buildings appropriate measures have been taken to protect the security of pupil's and staff information that is stored in onsite information systems, paper records, and cloud-based/online systems and in visual/audio media.

All staff must ensure that:

- personal data be kept in a locked filing cabinet, drawer, or safe; or
- if it is computerised, be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up; and
- be saved to the school server, school laptop/desktop or onto One Drive via a school account. Any removable storage is not permitted (this includes USB memory keys, portable hard-drives, SD cards, unencrypted laptops).

When staff are required to take personal information away from school sites, provisions have been made to support the secure transfer of information and guidance has been issued to staff who may be required to access personal data away from school.

Trust/School IT systems have appropriate security measures in place, with permission and access to personal information controlled based on the role and responsibilities of staff.

Paper records containing sensitive or confidential data are locked in secure storage spaces, with access controlled by the Head teacher at school and nominated appropriate staff at Trust level.

All staff are committed to ensuring that Personal Data held by school is maintained so that it accurate and of a quality that supports the purpose(s) it has been collected for.

Parents/carers are encouraged to support their school in the task of managing personal data for pupils by advising the relevant school office of any changes to personal information in a timely manner.

CCTV

CCTV is used at some of our schools to support the prevention and detection of crime. Where CCTV is used, this is stated on the schools Privacy Notice. We also notify staff, parents and visitors to school that CCTV is used via signage displayed in key points around the site.

Only designated staff at school or in the case of PFI schools, the PFI Company's designated employees, have access to view CCTV footage. CCTV recordings are kept for a period of time, after which the recordings are deleted/overwritten

Photographs and Digital Images (including video)

We use photographs and digital images for a variety of purposes across schools in the Trust, these include, but are not limited to:

- Capturing development and progress in learning
- School prospectuses and other publications focussed on promoting the school and Trust
- Assemblies and celebration events
- Sports day
- School performances
- Trips and residential outings

Where images of children or staff are used in public areas or made available online via publication on the school website, the school will always seek consent before images are published (see Appendices L and M).

Artificial Intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as Chat GPT and Google Bard. ECM Trust recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

If personal and/or sensitive data is entered into a generative AI tool in error or without proper permission/authorisation, ECM Trust will treat this as a data breach. The relevant supervisory authority will be notified and disciplinary action will be taken where and if appropriate.

Publication of School Information

Certain items of information relating to the school will be made available on the school website, in order to meet the legitimate needs of researchers, visitors and enquirers seeking to make contact with the school. Where it is not a legal requirement, personal data will not be published without consent from the individual concerned, or unless there is a legal requirement to do so.

Collection of data

All forms used by the school to collect personal data about a pupil will carry a standard Data Protection notice: as follows:

</We consent to the school (through the head as the person responsible) obtaining, using, holding and disclosing “Personal data” including “sensitive personal data” (such as medical information), for the purposes of safeguarding and promoting the welfare of our child, and where necessary, for the legitimate interests of the School and ensuring that all relevant legal obligations of the school and ourselves are complied with. / We give my/our consent to such processing and disclosure provided that at all times any processing or disclosure of personal data or sensitive personal data is done lawfully and fairly in accordance with the Data Protection Act 1998. >

The only exception to this is the letter that is sent out with a prospectus to a new enquirer. The following Data Protection notice should be inserted at the bottom of this letter:

< The personal data you supply to Every Child Matters Academy Trust will only be used in connection with your application for a school place. It will be held securely in line with the Data Protection Act and will not be passed to third parties. Every Child Matters Academy Trust is registered under the DP Act No ZA144772. See Appendix N

When Should Personal Data be rectified?

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

If the Trust/School has disclosed the personal data in question to third parties, The Trust/School must inform them of the rectification where possible. The Trust/School must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.

The right to erasure is also known as ‘the right to be forgotten’. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Under the DPA, individuals have a right to ‘block’ or suppress processing of personal data. The restriction of processing under the GDPR is similar.

When processing is restricted The Trust/School are permitted to store the personal data, but not further process it. The Trust/School can retain just enough information about the individual to ensure that the restriction is respected in future.

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

What is a Personal Data 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.

Example

A hospital could be responsible for a personal data breach if a patient's health record is inappropriately accessed due to a lack of appropriate internal controls.

What Breaches do The Trust/School need to notify the relevant supervisory authority about?

The Trust/School only have to notify the relevant supervisory authority of a breach where it is likely to result in a risk to the rights and freedom of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant social disadvantage.

This has to be assessed on a case by case basis. For example, you will need to notify the relevant supervisory authority about a loss of staff details where the breach leaves individuals open to identity theft. On the other hand, the loss or inappropriate alteration of a staff telephone list, for example, would not normally meet this threshold.

When do Individuals Have to be notified?

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, The Trust/School must notify those concerned directly.

A 'high risk' means the threshold for notifying individuals is higher than for notifying the relevant supervisory authority.

What Information Must a Breach Notification Contain?

- The nature of the personal data breach including, where possible:
- The categories and approximate number of individuals concerned; and
- The categories and approximate number of personal data records concerned;
- The name and contact details of the Data Protection Officer
- A description of the likely consequences of the personal data breach: and
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

How Do I Notify a Breach?

A notifiable breach has to be reported to the relevant supervisory authority within 72 hours of the organisation becoming aware of it. The GDPR recognises that it will often be impossible to investigate a breach fully within that time-period and allows you to provide information in phases.

If the breach is sufficiently serious to warrant notification to the public, the organisation responsible must do so without undue delay.

Failing to notify a breach when required to do so can result in a significant fine.

Staff must inform the Data Protection Officer immediately of any breach, who will then begin the investigation and being the notification process.

Retention and Disposal

The Trust operates a Retention Schedule to determine the length of time that documents containing personal data should be kept for. This schedule is in line with the recommended periods of retention published by the Information Records Management Society.

The school will also ensure that when obsolete, information is destroyed in a secure and appropriate manner. Records of destruction will be maintained where the disposal of personal data has been commissioned to third parties.

All paper documents that contain personal data will be shredded/incinerated once they are no longer required, accurate and up to date or when the retention period has been met.

Electronic devices containing personal data will be formatted and destroyed by an approved contractor with a certificate of destruction being presented for each disposal.

Audit

An audit of the schools compliance with this policy will be carried out on an annual basis by the Data Protection Officer in each school. This audit will be coordinated by the Data Protection Officer for The Trust or nominated person.

All schools must complete the Annual Data Protection Audit Return and forward this to the Data Protection Officer at the start of each autumn term (see Appendices O and P)>

All schools must test the Subject Access Request process in their school annually. This can be done by choosing a pupil at random and completing a S.A.R process sheet within the specified time detailing all the information gathered for that pupil. In line with the policy the process sheet will be forwarded to the Data Protection Officer for feedback and action.

Complaints

Complaints will be dealt with in accordance with the Trust's complaints policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

Review

This policy and related policies will be reviewed as it is deemed appropriate, but no less frequently than every 2 years. The policy review will be undertaken by the Board of Trustees.

Approved by the Board of Trustees on 24th September 2024.

To be reviewed Autumn Term 2026.



Chair



CEO

Contacts

If you have any enquires in relation to this policy, please contact the Head teacher who will also act as the contact point for any S.A.R's.

Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk or telephone 0303 123 1113.

Appendices

Appendix A	Privacy Notice Pupils
Appendix B	Privacy Notice Staff
Appendix C	Procedures for responding to subject access requests
Appendix D	Subject Access Request Form
Appendix E	Subject Access Request Release letter
Appendix F	Subject Access Request Process Sheet
Appendix G	Confidentiality and Data Protection (1)
Appendix H	Confidentiality and Data Protection (2)
Appendix I	CCTV Signage Advice
Appendix J	CCTV Operational Checklist
Appendix K	Small User Checklist Operation of CCTV System
Appendix L	Photography Consent Form
Appendix M	Parents who wish to use photography and / or video school event
Appendix N	Data Collection Sheet
Appendix O	Audit Outline
Appendix P	Audit Return
Appendix Q	Data Retention Guide
Appendix R	Disposal Log
Appendix S	Data Safety
Appendix T	Roles and Responsibilities



Privacy Notice for Pupils

ECM Academy Trust is a data controller for the Purposes of the General Data protection Regulation 2018 and as such is registered with the Information Commissioners Officer. We collect information from you and may receive information about you from your previous school.

Why do we collect and use pupil information?

We collect and use pupil information under the Data Protection Act 1998 (DPA) and “Article 6” and “Article 9” of the General Data Protection Regulation (GDPR).

Article 6 (GDPR) condition: processing is necessary for compliance with a legal obligation to which the controller is subject;

Article 9 (GDPR) condition: the data subject has given **explicit consent** to the processing of those personal data for one or more specified purposes

We use the pupil data to:

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

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

- Personal information (such as name, unique pupil number and address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information
- Relevant medical information
- SEN information
- Exclusions/behavioural information

We may also receive information from their previous school or college, local authority and the Department for Education (DfE).

Note: Schools and local authorities have a (legal) duty under the DPA and the GDPR to ensure that any personal data they process is handled and stored securely

For details of what we collect, hold and share, please visit the Information Commissioner's Office (ICO) Data Protection Register on <https://ico.org.uk/esdwebpages/search> and enter **Z9204596**.

Collecting pupil information

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

Storing pupil data

We hold pupil data in line with our Records Management Policy. After which this is securely disposed of by only using accredited data disposal companies.

Who do we share pupil information with?

We routinely share pupil information with:

- schools that the pupil's attend after leaving us;
- our local authority;
- the Department for Education (DfE);
- school nurse;
- EWO;
- Medical practitioners;and
- ECM Trust.

Why we share pupil information

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

We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our pupils with the (DfE) under regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

Data collection requirements:

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

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 Deb Barker on 01226 273220 or d.barker@ecmtrust.co.uk

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 to:-

Mrs D Barker
Data Protection Officer
Every Child Matters Academy Trust
Newsome Avenue
Wombwell
Barnsley
S73 8QS

01226 273220

d.barker@ecmtrust.co.uk

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:

Deb Barker on 01226 273220 or d.barker@ecmtrust.co.uk



Privacy Notice for School Workforce

Every Child Matters Academy Trust is a data controller for the Purposes of the General Data Protection Regulation 2018 and as such is registered with the Information Commissioners Officer.

We process personal data relating to those we employ to work at, or otherwise engage to work at, our school. This is for employment purposes to assist in the running of the school and/or to enable individuals to be paid. The collection of this information will benefit both national and local users by:

- improving the management of workforce data across the sector
- enabling development of a comprehensive picture of the workforce and how it is deployed
- informing the development of recruitment and retention policies
- allowing better financial modelling and planning
- enabling ethnicity and disability monitoring; and
- supporting the work of the School Teachers' Review Body and the School Support Staff Negotiating Body

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

- personal information (such as name, employee or teacher number, NI 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

We use school workforce data to:

- enable the development of a comprehensive picture of the workforce and how it is deployed
- inform the development of recruitment and retention policies
- enable individuals to be paid

We collect and use pupil information under the Data Protection Act 1998 (DPA) and "Article 6" and "Article 9" of the General Data Protection Regulation (GDPR).

- *Article 6 (GDPR) condition:* processing is necessary for **compliance with a legal obligation** to which the controller is subject

- *Article 6 (GDPR) condition:* processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller
- *Article 9 (GDPR) condition:* the data subject has given **explicit consent** to the processing of those personal data for one or more specified purposes

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.

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

- our 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 2017 and amendments
- The Department for Education (DfE) – We share personal data with the 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 workforce members with the DfE under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2017 and amendments
- HMRC for legal purposes

This data is stored for as long as is required under statutory requirements. Please see the school document retention policy for details of this. Any data is then disposed of using only accredited secure disposal companies.

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>

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 the Data Protection Officer, Mrs D Barker on 01226 206788 or d.barker@ecmtrust.co.uk.

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, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at <https://ico.org.uk/concerns/>

If you would like to discuss anything in this privacy notice, please contact:

Mrs D Barker on 01226 273220 or d.barker@ecmtrust.co.uk

Procedures for responding to subject access requests made under the GDPR 2018

Rights of access to information

There are two distinct rights of access to information held by schools about pupils.

1. Under the GDPR 2018 any individual has the right to make a request to access the personal information held about them.
2. The right of those entitled to have access to curricular and educational records as defined within the Education (Pupil Information) (England) Regulations 2005 (Pupil Information Regulations).

These procedures relate to subject access requests made under the GDPR 2018.

Processing a subject access request

1. Requests must be made in writing; and be addressed to the Head teacher. If the initial request does not clearly identify the information required, then further enquiries will be made.
2. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:
 - passport
 - driving licence
 - utility bills with the current address
 - Birth / Marriage certificate
 - P45/P60
 - Credit Card or Mortgage statement

(This list is not exhaustive).

3. Any individual has the right of access to information held about them. However with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Head teacher should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

4. The response time for subject access requests, once officially received, is 40 days **(not working or school days but calendar days, irrespective of school holiday periods)**. However any disclosure of personal data will not take place until after clarification of information sought.

5. The GDPR 2018 allows exemptions as to the provision of some information; therefore all information will be reviewed prior to disclosure.

7. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information, consent will be obtained where this is required. The 40 day statutory timescale will still be adhered to.

8. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another will not be disclosed, nor will information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

9. If there are concerns over the disclosure of information then additional advice will be sought.

10. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided will be retained in order to establish, if a complaint is made, what was redacted and why.

11. Information disclosed will be presented in a clear format, any codes or technical terms will be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it will be retyped.

12. Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant will be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail will be used.

Complaints

Complaints about the above procedures should be made to the Chair of the Board of Trustees who will decide whether it is appropriate for the complaint to be dealt with in accordance with the Trust's complaint procedure.

Complaints which are not appropriate to be dealt with through the school's complaint procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information

Contacts

If you have any queries or concerns regarding these policies / procedures then please contact Mrs D Barker on 01226 273220 / d.barker@ecmtrust.co.uk

Further advice and information can be obtained from the Information Commissioner's Office, www.ico.gov.uk or telephone 0303 123 1113

Subject Access Request Form

Request for information under the GDPR 2018

This form should be completed only if you are requesting personal information relating to yourself or on behalf of a third party.

Please complete in block capitals or type. (* *Required Fields*).

1. Personal details of the person requesting the information

Surname	
Forename	
Address	
Postcode	
Telephone Number	
Email Address	

2. Are you the Data Subject (i.e the person whose information you are requesting)?

Please tick the appropriate box

Yes

No

3. Personal Details of Data Subject (if different from those in section 1)

Surname	
Forename	
Address	
Postcode	
Telephone Number	
Email Address	
Date of Birth	
School Attended	

4. If you are not the Data Subject please describe your relationship with the Data Subject that leads you to make this request on their behalf

5. Information Requested

If you would like to see only specific documents please describe these below

6. If you would like a full copy of the personal records held by the school, please tick here .

Declaration

I certify that the information given in this application form to the school is true. I understand that it will be necessary for the school to confirm my/the Data Subject's identity and it may be necessary to supply more detailed information if required.

Signature (Person requesting the information)

Print name

Date:

GDPR 2018

The Data Controller is Every Child Matters Academy Trust (The Trust)

The details you provide on this form will only be used in connection with your application for the supply of documents and for statistical purposes.

The completed form should be returned to:

Data Protection Officer
Every Child Matters Academy Trust
Newsome Avenue
Wombwell
Barnsley
S73 8QS

I understand that I will receive acknowledgement of my request within 5 days of receipt. My request will be completed within 40 days in normal circumstances in accordance with the GDPR. However please note that The Trust will endeavour to complete your request as soon as is practical within this 40 day period

Office use only

Received by: Date:

Forwarded to: Date:

Date to be completed by:

Comments:

Appendix E: S.A.R. Release Letter

[Name]
[Address]

[Date]

Dear [Name of data subject]

GDPR 2018: Subject Access Request

Thank you for your correspondence of [date] making a data subject access request for [subject].

We are pleased to enclose the information you requested.

We have endeavoured to provide all the information that we hold on the data subject. However, if you have any reason to believe that there is any missing data then please do not hesitate to seek further clarity from us on this matter.

Yours Sincerely

SAR Process Sheet

SAR Reference					
Date Acknowledged					
Target Date to DPA					
Target Date for Release					
Verification of Subject					
Date	Description of document: letter/email /report inc who from / to and 'cc' details.	Editing done and reasons given. E.g. Third Parties anonymised	Notes – check names for editing	Copies Taken	Signature
Correspondence (sections within the file are noted)					
Emails					
SIMS					
Minutes of meetings					
Notes of Visits					
Student File					
CCTV					
Accident Book					
Staff Personal File					
Sickness Records					
Other					
Signature of DPA					
Date					

Confidentiality and Data Protection

Every Child Matters Academy Trust agrees to the service operating a confidential service on our premises. Discussions between individual pupils and staff of will remain confidential unless the young pupil of sufficient maturity* agrees to sharing, or there is an over-riding duty of care to the young person or someone else.

Pupils will be made aware of the confidential nature of this service by staff of at their interventions. Pupils will also be asked by staff of if, and what they may wish to share with the school, their parents or any third parties and their wishes will be respected.

Every Child Matters Academy Trust is registered with the Information Commissioners Office for Data Protection purposes. Every Child Matters Academy Trust takes the security of pupil data seriously and expects agency to implement appropriate security and other measures to safeguard pupils and their data in line with data protection legislation.

Confidentiality and data handling will form part of the review of this Service Level Agreement. Any concerns in this regard will be addressed by the personnel from each organisation.

Signed on behalf of Every Child Matters Academy Trust:

Name (please print):

Role:

Date:

Signed on behalf of:

Name (please print):

Role:

Date:

Confidentiality and Data Protection

Every Child Matters Academy Trust agrees to the service operating a service on our premises. Every Child Matters Academy Trust recognises that offers a confidential service in normal circumstances. However the service, when delivered on our premises, will be done so in line with the school's policy on confidentiality. The school will normally share information about the pupil's progress with the parent. It is only in exceptional circumstances where a conflict of interest may exist will the school consider withholding information. The service when working with pupils on our premises will adhere to this 'open' policy.

Discussions between individual pupils and staff of may be shared with the school and parents unless it is agreed that an exception can be made in a particular circumstance involving a pupil of sufficient maturity.*

Pupils/parents will be made aware of the open nature of this service by staff of at their interventions.

Every Child Matters Academy Trust is registered with the information Commissioners Office for Data Protection purposes. Every Child Matters Academy Trust takes the security of pupil data seriously and expects agency to implement appropriate security and other measures to safeguard pupils and their data in line with data protection legislation.

Confidentiality and data handling will form part of the review of this Service Level Agreement. Any concerns in this regard will be addressed by the personnel from each organisation.

Signed on behalf of Every Child Matters Academy Trust:

Name (please print):

Role:

Date:

Signed on behalf of

Name (please print):

Role:

Date:

Sufficient maturity*

The Information Commissioner would regard a young person age 12 to be of sufficient maturity to exercise their rights under the Data Protection Act. This includes the right to Consent or withhold consent to share. This is a general guide and it is recognised that some younger people may be sufficiently mature whereas some older people may not.

CCTV Signage Advice

All signs should be clearly visible and legible to members of the public. The size of signs will vary according to circumstances. For example:

- A sign on the entrance door to a building office may only need to be A4 size because it is at eye level of those entering the premises.
- Signs at the entrances of car parks alerting drivers to the fact that the car park is covered by such equipment will usually need to be large (probably A3 size) as they are likely to be viewed from further away, e.g. by a driver sitting in a car.

The signs should contain the following information:

- Identity of the person or organisation responsible for the scheme.
- The purposes of the scheme.
- Details of whom to contact regarding the scheme.

CCTV Operational Checklist

Introduction

This checklist is designed to help operators of small CCTV systems comply with the legal requirements of the GDPR 2018 and it details the main issues that need to be addressed when operating a CCTV system. When used as part of a regular review process it should help to ensure that the CCTV system remains compliant with the requirements of the Act.

It is important that the Data Protection Act is complied with because failure to do so may result in action being taken under this Act. Failure to comply with Data Protection requirements will also affect the police's ability to use the CCTV images to investigate a crime and may hamper the prosecution of offenders.

If you use a CCTV system in connection with your school you should work through the checklist and address all the points listed. This will help to ensure that your CCTV system remains within the law and that images can be used by the police to investigate crime.

Small User Checklist Operation of the CCTV System

This CCTV equipment and the images recorded by it are **controlled by** who is responsible for how the system is used and for the notifying the Information Commissioner about the CCTV system and its purpose (this is a legal requirement of the GDPR 2018).

The above controller has considered the need for using a CCTV system and has decided it is required for the prevention and detection of crime, for protecting the safety of the school and for the general running of the school. It will not be used for any other purposes.

Description	Checked (Date)	By	Date of Next Review
The controller is aware that notification to the Information Commissioner is necessary and must be renewed annually			
Notification has been submitted to the Information Commissioner and the next renewal date recorded			
Cameras have been sited so that their images are clear enough to allow the police to use them to investigate a crime.			
Cameras have been positioned to avoid capturing the images of persons not visiting the premises.			
There are signs showing that a CCTV system is in operation visible to people visiting the premises and the controllers contact details are displayed on the sign where it is not obvious who is responsible for the system.			
The recorded images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them.			
The recorded images will only be retained for 14 days to allow any incident to come to light (e.g. for a theft to be noticed).			
Recordings will only be made available to law enforcement agencies involved in the prevention and detection of crime, and no other third parties.			
The operating equipment is regularly checked to ensure that it is working properly (e.g. the recording media used is of an appropriate standard and that features on the equipment such as the date and time stamp are correctly set).			
Controller Knows how to respond to requests from individuals for access to images relating to that individual. See CCTV Code of Practice			

**Photograph/Video/Artwork/Activities
Consent and Release**

Occasionally we may take photographs of children at our school. We use these images as part of our school displays and class projects and sometimes in other printed publications and social media. To comply with the Data Protection Act we need your permission before we can photograph or make any recordings of your child.

Please complete and sign the form below, and return to the school.

I consent/do not consent (delete as appropriate) for my child's photograph or video image to appear on the school's website

I consent/do not consent (delete as appropriate) for my child's photograph or video image to appear on school displays and class projects. Occasionally we may wish to publish a name with a photograph on a school display only - I consent/do not consent for my child's name to be used on a school display.

I consent/do not consent (delete as appropriate) for my child's photograph or video image to appear on the school's facebook page.

I consent/do not consent (delete as appropriate) for my child's photograph to appear in the media.

I consent/do not consent (delete as appropriate) for my child to have a school photograph taken. I understand this printed/digital photograph can be purchased by parents.

I consent/do not consent for my child to use the internet in line with school's acceptable usage policy (policy shown on school website)

I consent/do not consent for my child to view film and video clips rated PG

I consent/do not consent for my child to take part in food preparation/cooking/tasting

I consent/do not consent for my child to attend supervised walks in the local area

Name of child:

Name of parent/guardian:

Signature of parent/guardian

Date:

Please note you may alter this consent at any point by completing a new form. Please note there is no detriment to your child if consent is refused.

Parents who wish to use photography and/or video a school event

Please note whereas this issue is not subject to the Data Protection Act schools need to have guidelines in place to cover such events. The following are guidelines which the schools might wish to adopt.

Generally photographs and videos for school and family use are a source of innocent pleasure and pride, which can make children, young people and their families feel good about themselves.

By following some simple guidelines we can proceed safely and with regard to the law. Remember that parents/carers and others, attend school events at the invitation of the Head teacher.

The Head teacher has the responsibility to decide if photography and videoing of school performances is permitted

The Head teacher has the responsibility to decide the conditions that will apply so that children are kept safe and that the performance is not disrupted and children and staff not distracted.

Parents and carers can use photographs and videos taken at a school event for their own personal use only. Such photos and videos must not be sold and must not be put on the public facing social media networks.

Recording or/photographing other than for your own private use would require the consent of all the other parents whose children may be included in the images.

Parents and carers must follow guidance from staff as to when photography and videoing is permitted and where to stand in order to minimise disruption to the activity.

Parents and carers must not photograph or video children changing for performances or events.

If you are accompanied or represented by people that school staff do not recognise they may need to check who they are, if they are using a camera or video recorder.

Remember that for images taken on mobiles phones the same rules apply as for other photography, you should recognise that any pictures taken are for personal use only.

In exceptional circumstances e.g. child protection orders the parent and Head teacher may agree an alternative and practical approach to this policy for specific pupils.

DATA COLLECTION FORM

Child's name		Date of Birth:	
Home address:		Post Code:	
Previous school / Nursery if applicable:			

Details of Parents/Guardians**Parent 1**

Full name		Priority *:	
Home address:		Post Code:	
Home telephone:	Mobile:	Day / Work Telephone:	
Email Address:		Parental responsibility? Yes / No	

Parent 2

Full name		Priority *:	
Home address:		Post Code:	
Home telephone:	Mobile:	Day / Work Telephone:	
Email Address:		Parental responsibility? Yes / No	

*Note - the priority order someone should be contacted in the case of an emergency in school

(ie: 1st, 2nd, 3rd, 4th etc)

The school runs a text message service. The Priority #1 contact will receive relevant messages in the event of an emergency or school closure. Please tick the box to confirm you **wish to receive SMS** text messages.

Emergency contact numbers alternative to parents/guardian

Emergency Contact 1 Relationship to child: _____

Full name		Priority *:	
Home address:		Post Code:	
Home telephone:	Mobile:	Day / Work Telephone:	

Emergency Contact 2 Relationship to child: _____

Full name		Priority *:	
Home address:		Post Code:	
Home telephone:	Mobile:	Day / Work Telephone:	

Emergency Contact 3 Relationship to child: _____

Full name			Priority *:	
Home address:			Post Code:	
Home telephone:	Mobile:	Day / Work Telephone:		

Do any of the following apply? Please attach a copy of legal document(s) if applicable

Adoption Court Order Residency Order
 Special Guardianship Any other Restrictions (please provide details)

Details of any other Restrictions:

Medical Information

Doctors	
Doctors address	
Doctors phone No.	

Medical conditions

My child has NO current medical needs

My child has a medical condition, or is undergoing investigations (please complete a **Medical Information Collection Form** available in school office).

Special Needs

Does your child have any special needs? Yes / No (please delete as appropriate)

Ethnicity

Country of birth: _____

Nationality _____

1st Language _____

Ethnicity

White British		White Irish		Other white background		M - white & black Caribbean	
M - White & Black African		M -White & Asian		M -any other		AAB -Pakistani	
AAB Bangladeshi		AAB - Indian		AAB - any other		BBB - Caribbean	
BBB - African		BBB - any other		Chinese		Arab	
Other ethnicity:	I do not want an ethnic background to be recorded						
M = Mixed AAB = Asian or Asian British BBB = Black or Black British							

Sibling information (if any)

Name	School
1.	
2.	
3.	

I/We consent to the school (through the head as the person responsible) obtaining, using, holding and disclosing "Personal data" including "sensitive personal data" (such as medical information), for the purposes of safeguarding and promoting the welfare of our child, and where necessary, for the legitimate interests of the School and ensuring that all relevant legal obligations of the school and ourselves are complied with. I/ We give my/our consent to such processing and disclosure provided that at all times any processing or disclosure of personal data or sensitive personal data is done lawfully and fairly in accordance with the Data Protection Act 1998.

Signature Date

Audit Outline

1. Aims of Data Protection Compliance Audits

- Mechanisms for ensuring that information is obtained and processed fairly, lawfully and on a proper basis.
- Quality Assurance, ensuring that information is accurate, complete and up-to-date, adequate, relevant and not excessive.
- Retention, appropriate weeding and deletion of information.
- Documentation on authorised use of systems, e.g. codes of practice, guidelines, etc.
- Compliance with individual's rights, such as subject access.
- To assess the level of compliance with the organisation's own data protection system.
- To identify potential gaps and weaknesses in the data protection system.
- To provide information for data protection system review.

2. Audit Objectives

When carrying out a Data Protection Audit in any area of an organisation the Auditor has three clear objectives:

- To verify that there is a formal (i.e. documented and up-to-date) data protection system in place in the area.
- To verify that all the staff in the area involved in data protection:
 - Are aware of the existence of the data protection system;
 - Understand the data protection system;
 - Use the data protection system.
- To verify that the data protection system in the area actually works and is effective.

3. Areas to be examined include:

- Use of appropriate forms when collecting data.
- Storage of data in accordance with the security policy, e.g. locked cabinets, passwords, etc.
- Data being removed in accordance with policy timescales.
- Subject Access Request process in place.
- CCTV compliance. Checklist completed and sent to the Data Protection Officer at Head Office.
- Staff training requirements assessed and highlighted.

Audit Return

School:

Date:

Description	Current Situation	Status	Action	Owner	Deadline
Staff/Pupil Records					
Student data is kept in accordance with the data retention policy					
Staff data is kept in accordance with the data retention policy					
Expired records are disposed of safely and securely by named individuals					
All forms used to collect data are identified					
All forms used to collect data include the standard ECM Data Protection disclaimer					
The pupil data collection sheet is sent out to parents annually at a set time to collect/refresh pupil data					
All electronic databases in use including the users who can access them are identified					
Access to all electronic databases is secured by individual username and password					
All paper record systems in use for staff or pupils are identified					
All paper systems are secured in					

accordance with policy guidelines					
Staff with access to staff records is documented controlled and regularly reviewed					
The accident book is used for pupils and records are kept for 40 years from the date the incident is logged					
All pupils whose parents have opted not to have their photograph used are clearly identified with the information easily accessible by staff					
All third party organisations offering a service on your premises including the data they collect are identified.					
All service level agreements with third party organisations are reviewed to consider data handling compliance.					
ALL CCTV Systems installed on your premises (if any) are documented.					
Appropriate CCTV signage is in place?					
The CCTV checklist is completed annually and returned to the data protection officer					
The school has a policy in place regarding the use of photography/video by family members at events. The method and frequency of communicating this to parents is					

documented and completed					
Contact details of parents are not distributed to other parents, for legitimate school activities, unless a signed parent Consent Form is received by the school					
A subject access request (SAR) file is in place to store requests					
THE SAR Process has been tested. Please complete Appendix D for a random pupil to test the process and outline any issues or concerns					
Staff Training					
Staff are made aware of ECM's Data Protection Policy and its implications for them in their work.					
Staff are made aware of ECM's acceptable use of ICT, mobile devices and networking sites policy and its implications for them in their work.					
Staff are made aware of that they must inform the school of any changes to their personal details e.g. change of address, contact numbers					
Have all staff had the minimum training session and been given the DO and Don't list? If not when is this planned?					

Status Key

Status	Description
	Policy Standard Not Met
	Policy standard partially met. Action plan in place to achieve full compliance
	Policy Standard achieved

Audit completed by (Print name):

Signed:

Position:

Date:

Data Retention Guide

1. Purpose of the Data Retention Guide

In the course of its activities every school creates and receives a large amount of information. Much of this information contains personal data which is in turn subject to the GDPR 2018 .

Personal data is any information relating to a living individual and would include information on pupils, members of staff and other employees. Data is very widely construed and can include internal files, letters, faxes, memoranda and notes, email, computer data and even voicemail, SMS and CCTV images created or received in the course of your operations.

This guide is intended to apply across the ECM group of schools to all data received and held whatever format that data is held in.

It is extremely important that data is held for the correct period of time so as to be available for the proper needs of the school. Indeed some classes of data are required by law or good business practice to be kept for a specified period of time and failure to do so may at best prejudice the position of ECM schools and at worst expose the group or its staff and employees to potential lawsuits and/or fines or even put them in contempt of court. However, keeping all data for an unlimited period of time will not only be impractical but will also expose ECM schools to risk under the DPA. This is because the retention of unnecessary data will create a compliance risk under the DPA as this requires that personal data is:

- Adequate relevant and not excessive;
- Accurate and up to date;
- Not kept for longer than is necessary

The excessive storage of data is not only highly obstructive to the smooth operation of the school but will also create a risk of prejudicing some or all of the above data protection principles.

The purpose of this guide is to provide guidelines for the retention, storage and disposal of the data held by the school.

2. Retention Periods

Except as otherwise indicated in accordance with paragraph 4 below data should be retained for the number of years indicated in the Retention Schedule below.

Each school will be responsible for the implementation of this guide. It is acknowledged that each school may currently have its own specific requirements and procedures for processing, storage and retention of data. These specific requirements and procedures should be reviewed against this guide to ensure that they are consistent with the procedures and time period specified in this guide. Any conflict or contradiction between a procedure which is specific to school and this guide should be discussed with the Data Protection Officer.

Where, in accordance with paragraph 4, it is necessary for a school to retain certain data for a period beyond the period indicated in the schedule, the school will maintain a flagging process to identify those records which must be retained beyond the specified period. The flagging process employed will be dictated by the records system in use.

Unless a flag has been given in respect of specific data then data should be destroyed as soon as practicable after expiry of the specified retention period.

3. Disposal of Records

A document which is to be destroyed in accordance with this guide is likely still to be sensitive in the wrong hands, to deal with confidential or personal matters and/or have other security implications. The method by which these types of documents are disposed is of importance both because of the inherent risk such material falling into the wrong hands and because in accordance with Principle 7 of the DPA, ECM schools has a legal duty to ensure that it is disposed of securely. The method of disposal of data shall be consistent with the type of data being destroyed. Confidential data should be disposed of in a way that prevents the data from being accessible to others.

The main disposal methods and safeguards are as follows:

- Secure destruction and recycling by specialised firms. The security of the service provider's methods should be fully investigated and guarantees built into any contract where possible.
- Shredding. For highly sensitive documents some types of shredding may not be sufficient and the waste may itself need to be destroyed in order to ensure that it cannot be pieced back together (this would be far more difficult if a quality cross-cut shredder was used). If shredding is done centrally, consideration may need to be given to the security of documents awaiting destruction.
- Incineration. Consideration will need to be given to environmental and other safety implications.
- Overwriting electronic data, or otherwise making it unreadable. Care needs to be taken to ensure that sensitive data is completely erased. For example, deleting a file on a PC may only delete the file reference and not the underlying data. With the right tools and knowledge, it is possible to reconstruct the file. Great care should also be taken to ensure the secure disposal of physical IT equipment upon which the personal data may have been held or processed.

4. Archiving data

In general once data or documents are no longer "live" they should be moved to archiving as soon as is reasonably possible. Archiving should not be confused with destruction. You need to keep in mind that archived data and documents carry with them on-going obligations and are subject to the requirements of the DPA, for instance, archived data and documents will need to be considered in the event of any subject access request and the archiving system must be kept properly secure.

Data and documents which have been archived should be reviewed against the criteria set out in this guide with a view to destruction after the relevant time period. Ultimately the archival period for data and documents is a matter of balancing costs of holding the data or documentation in archive which is highly unlikely ever to be needed against the general principle that everything else being equal, and it is better to be safe than sorry.

5. Retention of Data beyond the Retention Period

Where data should be retained indefinitely:-

- (1) If you receive notice of any lawsuit, government or regulatory investigation (for instance, health & safety investigations), other legal action, complaint or claim against or involving

ECM Schools, the School or any member of staff, or employee, or pupil or any of circumstances likely to give rise to such an action, proceeding, investigation complaint or claim, then you should flag all data which may be relevant for preservation in respect of the same. Any data so flagged shall be preserved and shall not be destroyed

(2) If any member of staff or employee becomes aware that any notice has been received by the school of any lawsuit, government or regulatory investigation, other legal action, complaint or claim against or involving ECM, the school or any member of staff, employee or pupil or any of circumstances likely to give rise to such an action, proceeding, investigation, complaint or claim, that member of staff or employee should immediately notify the school's Data Protection Officer in order that the Officer can review which data should be [flagged] for extended retention in accordance with this guide. The member of staff or employee must not destroy any data relevant to such action, proceeding, investigation, complaint or claim whether it not it would otherwise fall to be destroyed in accordance with this guide.

(3) If any member of staff or employee is unsure whether any unflagged data is relevant to an action, proceeding, investigation complaint or claim the member of staff or employee should not delete that data and should liaise with Data Protection Officer.

Once data has been flagged all members of staff and employees must preserve and prevent the destruction of any such data (including e-mails and other computer records).

Destruction of such data, even if inadvertent, could seriously prejudice the member of staff or employee, the school and ECM and could subject the individual, the school and ECM substantial criminal and civil liability including fines and other penalties.

Whenever data is flagged the data shall be preserved until the flag is removed. The communication imposing the [flag] shall be stored with the preserved data until that flag is removed, following which the data shall be destroyed as soon as reasonably possible.

6. Violations

Due to the potentially serious consequences of a violation of the procedures set out in this guide any violation may be subject to disciplinary action.

All members of staff or employees should report any suspected violations of this guide to the Data Protection Officer.

7. Questions

Anyone with questions about this guide should contact their *Data Protection Officer*.

Remember:

Data we record about individuals (staff, pupils, parents etc.) is covered by the Data Protection Act and belongs to that individual. As such, notes we make on SIMS, PORTAL, in emails and paper records may be seen by the person concerned.

We have access to data as part of our role within the school. This data should not be disclosed or used for any purpose that is not official business of the school.

The school has a data protection officer who can provide advice in case of uncertainty. Here is a list of 'top tips' when handling school data.....

DO ✓

- Record facts and professional opinions only, on school records, emails and other similar documents
- Use a strong password on I.T. Systems at work, e.g. a combination of 8 or more alphanumeric characters and symbols.
- Change passwords on a regular basis.
- Password protect email attachments containing personal or commercially sensitive data.
- Encrypt any removable data devices including USB sticks laptops and similar.
- Remember the school may incur substantial fines for loss or misuse of data.
- Read and familiarise yourself with the Acceptable Use Policy (I.T.).
- Keep data secure when using it off site.
- Think security when posting sensitive documents.

DON'T x

- Use personal social media with pupils.
- Contact pupils or store pupil/parent contact data on personal devices, e.g. numbers on your mobile.
- Use your mobile phone outside designated areas in school.
- Don't share passwords.
- Don't leave personal data unattended when off site.
- Don't create databases of Personal Data in addition to the official sources e.g. SIMS and PORTAL.

Taking data off site.

- only take offsite, information you are authorised to and only when it is necessary.
- ensure that it is protected offsite by not leaving it unattended,
- locking it away when not in use,
- not discussing or sharing it with non-school staff.
- be aware of your location and take appropriate action to reduce the risk of theft
- make sure you sign out completely from any online services you have used e.g. email
- try to avoid other people seeing the information you are working with
- treat records as if they were your bank details and PIN

Disposal Log

Date	Description	Records Included	Exception
	<i>Example: Annual audit of records in line with retention timescale or request from subject to change or delete record</i>	<i>Records reaching D.O.B + 25 year rule</i>	<i>Individual Pupils Record as per retention log e.g. for legal proceedings ongoing etc.</i>

Roles and Responsibilities

Role of the Data Protection Officer

The role of the Data Protection Officer is to:

- Ensure that the organisation complies with the GDPR 2018, and to ensure that employees are fully informed of their own responsibilities for acting within the law and that the public, including employees, are informed of their rights under the Act.
- Be the nominated officer in the Data Protection register maintained by the Information Commissioner, notify the fact of processing to the Information Commissioner and maintain the accuracy and currency of the organisation's notification
- Co-ordinate Data Protection Act activities (including training) and facilitate such user group meetings as necessary e.g. Data Protection Coordinator's group
- Ensure organisational compliance, and conformance with the Data Protection Principles
- Develop, implement and enforce a suitable and relevant Data Protection policy and ensure it is reviewed on an annual basis
- To undertake systematic Data Protection Act compliance audits in accordance with Information Commissioner's audit tool
- Assist with investigations into complaints about breaches of the Act and undertake reporting/remedial action as required. Maintain a log of any incidents and remedial recommendations and actions.
- Maintain a log of and co-ordinate Subject access requests.
- Maintain and update own knowledge of developments in Data Protection issues.
- Be a resource for other employees by providing expert advice on the Data Protection Act and related issues.

Role of the Head teacher

- The Head teacher is responsible for the successful implementation of this policy in their school. The Head teacher will agree and authorise all data to be released in connection with a S.A.R. (Subject Access Request)