THE ECCLESBOURNE SCHOOL

Learning Together for the Future

DATA PROTECTION POLICY (GDPR)

March 2023

This policy should be updated annually, it will next be updated March 2024

Contains information also on Protection of Children's Biometric Information

This is a statutory policy

Contents

1 Background & Definitions 3
2 Policy Statement 3
3 Roles and Responsibilities 4
4 Scope of the Policy 5
5 Management of Data 6
6 Information stored on pupils/Parents and Carers. 7
7 Specific Data Risk Areas 8
8 Off Site Working 9
9 Authentication & Workstation Locking 9
10 Monitoring 9
11 Non Compliance 10
12 GDPR and Data Protection Training 10
13 Requests and charges 11
14 Review and appeal 11
Appendix 1 – Withdrawal Of Consent Form (Individual) 12
Appendix 2 - Consent Withdrawal Form – on behalf of Pupil 13

1 Background & Definitions

What is the GDPR?

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

The current Data Protection Act 1998 has been repealed and replaced with the Data Protection Act 2018.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

2 Policy Statement

The Ecclesbourne School Academy Trust is committed to the principles of the Data Protection Act 2018 incorporating the European Union General Data Protection Regulation (GDPR). These Principle state data should be:

Processed with 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'.

Collected for a specific purpose and used for that purpose only

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 in 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.

Accurate

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 no longer be held by the Controller or should not be held by the Controller. A dispute resolution process and complaint process can be accessed, using the suitable forms.

Retention for a specified period

School has a retention policy that explains how long we store records for. This is available on request/on the website. The school also has a retention policy that specifies clearly what documents we keep, how we keep them for and the purpose we keep them.

Stored Securely

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

Our Commitment

This statement represents the response of The Ecclesbourne School Academy Trust to its duties under the Data Protection Act 2018.

Aims

The Ecclesbourne School Academy School will implement the requirements of the Data Protection Act 2018 and Data Retention Regulations 2009 and any subsequent amendments or regulations on protecting data, and the academy's controls and procedures will ensure integrity and security of data.

The Ecclesbourne School Academy School will maintain a Data Protection register entry with the Information Commissioner, and ensure that all personal data obtained, held, used or disclosed conforms to the details recorded within that registration.

In addition, The Ecclesbourne School Academy School will ensure that:

- The Director of Learning Services has overall responsibility for the implementation of Data Protection.
- All staff are aware of their responsibilities under the Data Protection Act.
- All staff are aware of their responsibilities under the Data Retention Regulations.
- Staff are trained and supported to deal effectively with the requirements of the Act, including the need to deal with subject access requests, in whole or in part, in accordance with the Act.
- The requirements of the Act are considered in decision making processes, such as the development of policy and procedures and the design and the implementation of information systems.
- The operations of the organisation are developed to meet the highest standards of openness and accountability.

3 Roles and Responsibilities

The Data Protection Act 2018 & GDPR outlines the following roles:

Data Protection Officer

The role of Data Protection Officer must be carried out by someone attached to or appointed by The Ecclesbourne School who does not directly process any data. 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

The School has appointed John Walker of J. A. Walker Solicitor to carry out the duty of DPO on our behalf.

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.

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.

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 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 subject's 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.

4 Scope of the Policy

The policy statement of commitment and the ensuing controls and procedures arising from the policy are applicable to all employees of the Trust, including students, Governors and Trustees. Those with responsibility for handling or processing information are particularly affected.

5 Management of Data

Data Collection & Processing

School 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 management plan of how school will respond to this. This forms part of our risk management process.

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.

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.

The information will be supplied in an electronic form.

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

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 school will follow its processes as outlined in the risk management plans.

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.

6 Information stored on pupils/Parents and Carers.

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.

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

Withdrawal of Consent

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

If you wish to withdraw consent then you must inform the school in writing.

7 Specific Data Risk Areas

CCTV Usage

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

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

All Staff, contractors and third parties who have control over lockable areas have a responsibility to 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 GDRP and DPA compliance.

- Server Hardware is disposed of and recycled by Enviro Electronic. Client Hardware is disposed of and recycled by Enviro Electronic
- Hard copy files are destroyed by Veolia
- Portable and removable storage are destroyed / cleaned/ recycled by Enviro Electronic

Biometrics

Biometric data is personal information about an individual's physical or behavioural characteristics that can be used to identify the person. In school we only use a person's fingerprints for recognition. As a school we do not store any images of the individual's full fingerprint.

The school operates biometric recognition systems for:

- Cashless Catering

All data collected will be processed in accordance with the GDPR Data Protection Principles and the Protection of Freedoms Act 2012.The written consent of at least one parent will be obtained before biometric data is taken and used. If one parent objects in writing, then the school will not take or use a child's biometric data.

8 Off Site Working

Staff are often provided with devices to enable them to complete their duties away from the school site. This presents a significant risk of data breach.

Laptops

All School owned laptops that are loaned to staff members must have Drive Encryption enabled. This drive encryption must protect the system disk or any other storage disk inside the device

Mobile Phones & Tablets

All Mobile phones will be encrypted using inbuilt device encryption and must use unlock patterns to secure against unauthorised access. School owned mobile devices must be tracked using an MDM solution allowing them to be remotely wiped.

Remote Desktop

Remote desktop is in operation to facilitate off site working whilst maintaining data security. Using remote desktop reduces the amount of data that is required to be taken offsite.

Whilst technical solutions can mitigate much of the risk staff members must be made aware of their responsibilities regarding Data Protection and portable equipment.

9 Authentication & Workstation Locking

Password Complexity

Unauthorised access through unsecure passwords present a significant risk. For this reason, password complexity requirements are enforced for all administrative users. These rules are

Workstation Locking

All Administrative workstations are subject to auto lock where their systems will automatically lock after a 5-minute period of inactivity. Classroom-based computers connected to projection equipment are exempt from this rule as the timeout would severely hamper the core business of teaching. In this instance it is the responsibility of the member of staff concerned to lock the workstation as and when it is not in use or when leaving the room where the device is located.

Data Portability

The GDPR requires an organisation that stores data to enable transfer of that data from one organisation to another. In schools, pupil data is transferred using the Common Transfer File (CTF) which is a DfE standard process. This is outside the scope of data portability in the GDPR.

Employee data will be shared to enable new starters and leavers to take up new roles as easily as possible.

When new data is provided to school it will then be administered and processed within the terms of the Data Protection and any other relevant policy.

10 Monitoring

The Deputy Head Learning Services will maintain a register of all requests made for information under the Data Protection Act that do not fall within the remit of the Data Protection Registration with the Information Commissioner, and the action taken on each application. It will identify reoccurring requests for the same or similar information and provide information for the reviews of the Data Protection Registration.

The Ecclesbourne School Academy will register all complaints received about its Data Protection arrangements and will ensure learning points that arise from such complaints are used to improve related policies, procedures and guidance.

The Deputy Head Learning Services will review this policy and its associated procedures and arrangements every two years to ensure it remains up to date, effective and takes account of emerging good practice. Where new legal directions come into force, the policy will be reviewed in line with the commencement of that legislation.

The Director of Finance will ensure that the Trust's Data Protection Registration is renewed, reviewed and, where necessary, updated annually.

Criteria for monitoring

The Policy and associated procedures and arrangements will be monitored within the context of legislation, including:

- Data Protection
- Data Retention
- Computer Misuse
- Human Rights
- Equal Opportunities
- Telecommunications
- Health & Safety

11 Non Compliance

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.

12 GDPR and Data Protection Training

The Ecclesbourne School wants 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 staff This will be for employed staff and volunteers.

13 Requests and charges

Requests should be made in writing by letter or email to the Deputy Head Learning Services:

The Ecclesbourne School Academy Trust
Wirksworth Road
Duffield
Derbyshire
DE56 4GS

Proof of identity (normally a driving licence, passport or utility bill or corporate identification in the case of organisations) will be required before the request can be met.

The request will be dealt with within the required response time of 40 calendar days, subject to any extensions as stated within the Data Protection Act.

If the request is too general the Trust will offer advice and assistance to determine the information required. The Trust does not have the right to ask why information is being sought, but the information can be volunteered to assist the Trust in meeting the request.

The Trust will provide specific charges for the copying of information dependent on the amount of information required.

14 Review and appeal

If an applicant is dissatisfied with the handling of a request, they have the right to ask for an internal review. Internal review requests should be submitted no later than 40 working days after the date on which the applicant believes that the Trust has failed to comply with the requirement, and should be addressed to:

The Chair of Governors
The Ecclesbourne School Academy Trust
Wirksworth Road
Duffield
Derbyshire
DE56 4GS

If not content with the outcome of the internal review, an applicant has the right to apply directly to the Information Commissioner for a decision. The Information Commissioner can be contacted at: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

Appendix 1 – Withdrawal Of Consent 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 The Ecclesbourne 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 staff member:

Appendix 2 - 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 The Ecclesbourne School to process their 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 staff member:

Dated:

Actions: