Esh Winning Primary School

Data Protection Policy

October 2023
Review: October 2024

Table of Contents

Note: Within this policy the term "company" refers to Esh Winning Primary School.

1. Revision History

The below table provides the revision history for this document. Each revision has an associated date, issue number, and description of the changes and/or content. The document revisions appear in descending order, with the most-recent iteration appearing first in the table.

Date	Version	Description	Author

2. Document Approval

Document Name	Data Protection Policy
Publication Date	October 2023
Prepared by	Data2Action & Esh Winning Primary School
Approval (Name & Organisation)	Governor Finance, Premises and Staffing Committee

1. Purpose

The purpose of this Policy is to apply the principles of the Data Protection Regulations and to ensure all employees (including temporary, casual or agency staff) and contractors, consultants and suppliers working for, or on behalf of, the company and who process personal data on behalf of the company, understand the requirement to comply with Data Protection Legislation. Personal data processed by the company includes that related to our clients, employees, associates, contractors and any other identifiable living individual.

The UK General Data Protection Regulation (UK GDPR) is implemented in the UK by the Data Protection Act 2018.

The company strives to ensure it delivers fair outcomes for clients and employees and shall never knowingly or intentionally breach any applicable law or regulation relevant to the conduct of its activities. The company is committed to the highest standards of ethical conduct and integrity in its activities and is dedicated to acting in an open and honest manner. The company's employees and associated third parties should always comply with the spirit of this Policy, the overriding objective of which is to protect Personal Data held by the company.

This Policy does not contain an exhaustive set of requirements and should therefore be read in conjunction with the wider suite of data and information security policies which exist to provide a structure for employees to work within and remain compliant with all relevant legislation.

2. Scope

The company is required by law, and to perform its function, to collect and use certain types of information. This personal information must be dealt with lawfully and correctly whether it is collected, recorded and used on paper, information technology or other material. This includes information on current, past and prospective students and employees, suppliers, service users and others with whom it communicates with including:

- Personal data processed by the company;
- Personal data controlled by the company but processed by another third party, on the company's behalf (for example payroll provider);
- Personal data processed jointly by the company and its partners;

Personal data held by the company may be held in many forms including:

- Database records;
- Computer files;
- Emails;
- Paper files;
- CCTV and video recordings;
- Sound recordings;
- Photographs;
- Website;
- Mobile phones.

Data subjects may include:

- Current, past and prospective employees, associates, contractors;
- Clients;
- Suppliers;
- Service users;
- Others with whom the company communicates.

This policy provides outline measures and puts in place a structure for monitoring compliance.

3.Risk Appetite

The company has no appetite for regulatory breaches. The company has a very low risk appetite to breaches of this policy and related procedures.

4. Policy Statement

4.1 Data Protection Regulations

At the time this policy was written, it aims to satisfy data protection and associated regulations in the United Kingdom which include:

- The UK General Data Protection regulations (UK GDPR)
- The UK Data Protection Act 2018
- Privacy in Electronic Communications Regulations (PECR) 2003, updated in the e-privacy bill on 25th May 2018
-

The UK General Data Protection Regulation (UK GDPR) governs how information about individuals should be treated. It also gives rights to individuals whose data is held. The Regulation came into force on 25 May 2018 and applies to all personal data collected at any time whether held on computer or manual record.

This policy will be updated in accordance with any changes made to the afore mentioned Regulations.

Data Processing in the UK is regulated by the Information Commissioners Office (ICO). The company is registered with the ICO as a Data Controller, registration {insert}.

The company has appointed the following Data Protection Officer (DPO) who is the central point of contact for all **data protection related** matters;

DPO: Gillian Welsh

Company: Data2Action

Email: info@data2action.co.uk

Telephone: 0333 202 6397

Company Registered Address: Suite 2e, Business & Innovation Centre, Silverbriar, Sunderland, SR5 2TP

4.2 The GDPR Data Protection Principles

There are 7 Principles relating to the processing of personal data which the company must comply with:

1. **Lawfulness, Fairness and Transparency –** Data should be processed lawfully, fairly and in a transparent manner in relation to the data subject;

2. **Purpose Limitation –** Data should be collected for specified, explicit and legitimate purpose and not further processed in a manner that is incompatible with those purposes;

3. **Data Minimisation -** Data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4. **Accuracy –** Data should be accurate and where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purpose for which they are processed, are erased or rectified without delay;

5. **Storage Limitation –** Data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed;

6. **Integrity and confidentiality –** data should be 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;

7. **Accountability –** the data controller must be responsible for and be able to demonstrate how it applies principles 1 to 6.

4.2.1 Lawfulness, Fairness and Transparency

4.2.1.1 Lawful basis for processing personal data

Processing of personal data is **only permitted** if one of the following applies;

- It is done with the expressed **consent** of the data subject
- It is necessary for the provision of service or the performance of a **contract**
- It is necessary for compliance with a **legal action**
- It is necessary to protect the **vital interests** of the data subject or another natural person
- It is necessary for the performance of a task carried out in the **public interest**
- It is necessary for the purpose of the **legitimate interests**. When using the lawful basis of Legitimate Interest, a 'Legitimate Interest Assessment' (LIA) should be completed to ensure that the interest is demonstrable.

4.2.1.2 Data Subject Consent Requirements

Where processing is based on consent, the company must be able to demonstrate the data subject has consented to processing of personal data. Any consent must be freely given, which means that the company cannot make the provision of any services or other matter conditional on a **data subject** giving their consent.

In the UK, the regulation stipulates that any person aged 13 or over has the right to give their consent, therefore, at this age it is not the parent's consent but the child's that is generally required. It may be however that the child is not able to fully understand the context or extent of the consent and as such, it may be appropriate to also seek consent from the parent. For further support on this please refer to the company DPO.

If the data subject's consent is given in the context of a written declaration, which also concerns other matters, the request for consent must be presented in a manner that is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language.

The data subject must have the right to withdraw their consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. A record must always be kept of any consent, including how and when it was obtained.

4.2.1.3 Special category data and explicit consent

Processing of data revealing ***racial*** or ***ethnic origin***, ***political opinions, religious or philosophical beliefs, or trade union membership*****,** and the processing of ***genetic data***, ***biometric data*** for the purpose of uniquely identifying a natural person, data concerning ***health*** or data concerning a natural persons ***sex life or sexual orientation*** is generally prohibited, but where this processing is vital, it must only be carried out with either the **explicit consent** of the data subject or in fulfilment of other conditions and set out in Article 9 of the regulation. A record of the explicit consent must be retained.

4.2.1.4 Transparency

The company outlines its obligation to inform data subjects via it's Privacy Notice which is located on the company website for external reference. Data subjects in the context of the company include employees of clients, customers and employees, associates or contractors.

The Privacy Notice may also be provided where there is a specific activity which requires the collection and processing of personal data. Therefore, at the point where personal data relating to a data subject is collected, the company must, at the time of collecting the personal data, provide the data subject with the following information;

- The identity and contact details of who is collecting the data e.g. {company};
- The contact details of the Data Protection Officer (DPO);
- The purposes of the processing as well as the legal basis for processing;
- The third-party recipients or categories of recipients;
- The period for which the personal data will be stored;
- The existence of the right for the data subject to:
    - Be informed
    - Request access to their data
    - Rectification
    - Erasure
    - Restrict processing

    - Object to processing
    - Data portability
    - the existence of any automated decision-making, including profiling, as well as the significance and the envisaged consequences;
- The data subjects right to lodge a complaint with a supervisory authority (ICO);
- The lawful basis or processing
    - Where processing of data is based on consent, the existence of the data subjects right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal. This is particularly relevant where a child's data is obtained where parental consent may have been obtained, the child has the right to withdraw this consent;
    - Where the processing is based on legitimate interests, what the interest is.

4.2.2 Purpose Limitation

The company and its employees must only collect and process personal data for the purpose specified at the point of collection. When the data is used for a purpose other than for which it was collected, the company must provide the data subject with confirmation of this, prior to any further processing.

4.2.3 Purpose Minimisation

The company will collect, process and create records containing personal data only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements. Such processing or creation of records will:

- Enable employees to do their work consistently in full knowledge of the processes, decisions and actions that inform and drive the delivery of our services;
- Ensure the availability of credible and authoritative evidence to protect the rights of the company, its employees and clients;
- Demonstrate accountability by providing the evidence and information required for any internal or external audit;
- Ensure that all records are up to date and accurate;
- Make sure that only relevant data is captured, and the personal data obtained is not excessive.

4.2.4 Data Accuracy

Personal data processed by the company must be accurate and kept up to date at all times. All reasonable steps must be taken to ensure that personal data that is inaccurate is erased or rectified without delay. Data subjects have the right to have any inaccurate data corrected at any time.

4.2.5 Storage Limitation

4.2.5.1 Data Retention and Destruction

The company's Data Retention Schedule must be adhered to at all times, retaining data for longer than is necessary would constitute a breach of the regulation. Data owners must determine and document processes for ensuring the data retention schedule is adhered to and that data is disposed of accordingly once it reaches the end of its retention period. Processes should include how these practices are monitored.

Confidential and personal data must be securely and permanently deleted or disposed of once the retention requirements have been reached and must be disposed of in a way that protects the rights and privacy of data subjects.

All confidential and personal data is to be shredded and disposed of as 'confidential waste'. Hard drives and portable media must be disposed of securely using approved third parties as necessary.

4.2.6 Integrity and confidentiality – Data Security

4.2.6.1 Access and Storage

The company shall implement appropriate security, technical and organisational measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Example measures to ensure the level of security appropriate to risks of processing personal data include:

- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- Maintain a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of Data Processing;
- The pseudonymisation and encrypting of data when and where appropriate.

Recommended security procedures include:

- **Entry controls.** Awareness within the company to report any stranger seen in entry-controlled areas to a Line Manager.
- **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.). It is the individual responsibility of every employee to clear their desk or work area of any confidential information (which includes any information relating to an identifiable individual).
- **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required. IT assets must be disposed of in accordance with the applicable policies.
- **Equipment.** Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.
- **Working away from the company premises – paper documents.** Employees are discouraged from removing paper documents containing confidential information from company premises. However, where this is absolutely necessary, measures need to be put in place to ensure security of the documents. They must not be left in an unattended vehicle, not worked on in public and if taken home they must be secured in a locked cupboard until returned to school.
- **Working away from company premises – electronic working.**
  Employees can access the company network securely from a remote device and when doing so the same security precautions much be taken. USB sticks are prohibited unless encrypted and documents must not be downloaded and stored in personal folders if they contain any personal data attributable to an individual student or employee.
- **Document printing.** Documents containing personal data must be collected immediately from printers and not left on photocopiers.

- **Telephone, radio (where applicable) or discussions** in person relating to any confidential matter in respect of an identifiable individual must take place in private and not be overheard.

An employee must only access personal data they need to use as part of their job and where they have been authorised to do so. Inappropriate or unauthorised access may result in disciplinary action, including dismissal and criminal prosecution.

All employees are responsible for ensuring that confidential and personal data held by the company is stored securely against unauthorised or unlawful loss or disclosure.

Manual files and other records or documents containing personal/sensitive data will be kept in a secure environment and accessed on a need-to-know basis only.

Personal data held on computers and computer systems will be installed with user-profile type password controls, encryption and where necessary, audit and access trails to establish that each user is fully authorised. Personal data should not be held on unencrypted electronic devices. Security arrangements will be reviewed regularly, any reported breaches or potential weaknesses will be investigated and, where necessary, further or alternative measures will be introduced to secure the data.

Confidential or personal data must not, under any conditions, be disclosed to any third party, unless that third party has been specifically authorised by the company to receive that information and has entered into a **Data Processing Agreement (DPA)** with the company or has been specifically authorised by the data subject themselves.

Confidential or personal data displayed on computer screens and terminals must not be made visible except to authorised employees and the data subject themselves.

Confidential or personal data must not be removed from the company premises unless necessary and with approval of the Headteacher. Personal data will not be transferred outside the UK/European Economic Area without appropriate contracts and approval.

4.2.6.2 Anonymisation Requirements

Anonymisation is the process of turning data into a form which does not identify individuals and where identification is likely to take place.

Personal data must be anonymised if it is to be used for a purpose other than which it was collected when consent was obtained (e.g. data analysis, system testing or training).

4.2.7 Accountability

The company takes its accountability very seriously and as such ensures appropriate organisational and technical measures are implemented and reviewed continually.

4.2.7.1 Training

All relevant employees will undergo training which outlines their responsibilities under this Policy. company employees will undergo this training on induction into the company and subsequent additional refresher training on a regular basis.

4.2.7.2 Documentation

The company maintains evidential documentation in demonstration of its compliance with the Regulation. This includes Records of Processing, Policies, Procedures and logs. All documents are subject to a review period and are trained to employees who have access to them, as appropriate, through the company's internal intranet/ shared access folders.

4.2.7.2.1 Records of Processing

Where the processing of personal data is of a high volume or high-risk nature then the company will maintain a Record of Processing detailing activity under its responsibility containing the following information;

- The name of the contact details of the company (and where applicable the Joint Controller, the controller's representative and the Data Protection Officer)
- A description of categories of the data subjects and categories of personal data
- Classification and handling of data
- The lawful basis for processing
- Any 3rd party processing and 3rd country transfers

These records are to be made available to the Information Commissioners Office (ICO) on request.

4.3 Data Privacy by Design (and default)

The GDPR requires the company to integrate data protection concerns into every aspect of our processing activities. This approach is 'data protection by design and by default'. It is a key element of the GDPR risk-based approach and its focus on accountability, i.e. our ability to demonstrate how we are complying with its requirements.

4.3.1 Data Protection Impact Assessment (DPIA)

This is a process to help identify and reduce the data privacy risks of a project or a change and should be completed at the outset and throughout the development or implementation of a project / change;

- It enables the company to analyse how a project or a change may affect the privacy of individuals involved systematically
- A DPIA should be applied to new projects to allow greater scope for the project needs to be implemented and should also be used when planning changes to an existing system or BAU process.
- The DPIA should ensure privacy risks are minimised whilst allowing the project / change to meet its objectives
- Risks can be identified early in the project / change by analysing how data will be used (risks to data subjects such as potential for damage or distress)
- The DPIA should also assess the risks to the company such as the financial and reputational impact of a breach arising from the project (higher risk projects that are likely to be more intrusive are likely to have a higher impact on privacy

The DPIA process should not need to be overly complex or time consuming, but there is an expectation of a certain level of rigour in proportion to the privacy risks arising from the process or project under review. The company has a documented process and DPIA template which should be used. The DPO should always be consulted as to whether a data protection impact assessment is required, and if so how to undertake that assessment as well as being part of the final sign off process.

4.4 Data Subject Rights

The company must maintain appropriate procedures to facilitate data subjects exercising their rights and will not refuse to act on such a request, unless the company cannot confirm the identity of the data subject.

Data subjects have the rights to:

- Be informed
- Access the information we hold about them (Data Subject Access Request Procedure)
- Have their details rectified if inaccurate
- Have their details deleted if they are not required for lawful reasons
- Object to their data being processed
- Request the processing of their data restricted
- Have automated processing and profiling restricted
- Request information processed by automated means is sent to them (or another nominated Data Controller) in a commonly used electronically readable format

4.4.1 Subject Access Requests (SARs)

The company will provide individuals with a copy of the information held about them within one calendar month of receiving a request. On receiving such a request, the company must check and require evidence to determine the identity of the individual and any further information required to clarify the specifics about the request being made.

Where a subject access request has a broad scope, the company may ask for more details from the data subject in order to locate the specific information that is of interest. Where a large volume of information is held, the company may seek to make the information available in ways other than providing a copy.

The company has (and will maintain) an appropriate Subject Access Request Process in place that should be referred to in conjunction with this policy. All Subject Access Requests received will be recorded for monitoring and reporting purposes on the appropriate log.

Requests from individuals to correct, rectify, block, or erase information that they regard as incorrect or to stop processing that is causing damage or distress will be considered by the company on a case by case basis. The individual concerned will be fully informed of the resulting decision and the reasons for it.

Data subjects should be able to make SARs and exercise their rights easily and at no cost.

4.5 Data Sharing / Third Party Processing

4.5.1 Sharing with Third Parties

Personal sensitive data will not be shared unless it is in connection with the primary purpose for which the information was collected, or the data subject has explicitly given their permission for the information to be shared for this purpose, or another legal provision (GDPR exemption exists) to allow the sharing such information.

The company will ensure that supporting processes and documentation are made available so that they understand how to share information safely and lawfully.

Any data sharing with third parties must be done only in agreement with senior leaders or DPO.

4.5.2 Third Parties

The company may choose to use a third party to provide a service or a product and this may include access to some records. This does not dismiss any responsibility for the safety and security of these records.

Examples of various organisations who may provide services to the company include;

- Payroll provider
- Recruitment providers
- Online payment systems
- Online Software as a Service systems

The company will only choose third parties who provide sufficient guarantees about how they will protect these records and will ensure due diligence is completed along with written and enforceable contracts (Data Processing Agreements/ DPA).

All contractors who are users/processors of personal information supplied by the company will be required to confirm that they will abide by the requirements of the Regulation to the same standard as the company.

All third parties to the company must ensure they, and all of their staff who have access to personal data, held or processed for or on behalf of the company, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the Regulation. Any breach of any provision of the Regulation will be deemed as being a breach of the contract between the company and that third party. The company shall take reasonable steps to ensure regular monitoring of contracts and specifically the security of data being processed on its behalf and must allow data protection audits by the company if requested, in line with these contractual arrangements.

Any observed or suspected security incidents or security concerns should be reported to the Headteacher or DPO immediately in line with the GDPR Data Breach Process.

Third parties will not be able to sub-contract Data Processing without the explicit written permission of the company.

4.5.3 Joint Controllers

Where two or more controllers jointly determine the purpose and means of processing, it is referred to as being 'Joint Controllers'. Where this is the case, the company and the other Joint Controller shall in a transparent manner determine their respective responsibilities for compliance with the Data Protection Regulations, in particular with regards to exercising the rights of the data subject and their respective duties to provide the information and gain consent. In these situations, documented contracts are required by way of a Data Sharing Agreement (DSA).

4.6 Data Breaches

All data breaches (however minor) should be reported via the process detailed in the company GDPR Data Breach Process.

The definition of a personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

A personal data breach may (if not addressed in an appropriate and timely manner) result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.

Therefore, as soon as anyone within the company becomes aware of a personal data breach this should be considered very seriously and acted upon immediately.

All personal data breaches must be reported in line with the procedure without undue delay (and not later than 72 hours after having become aware of the breach).

4.6.1 Complaint Handling Requirements

Processes and procedures are in place and maintained for handling complaints relating to Data Protection. The relevant Line Manager and DPO must be notified of any upheld complaints relating to data protection and must be kept informed of any correspondence with the individual making a complaint.

5 Policy Governance

Monitoring to assess the adherence to and effectiveness of this policy will be completed periodically by the DPO and Governors.

Monitoring should be conducted on a regular basis, but no less than once annually.

5.1.1 Roles and Responsibilities:

First line of audit

All Employees

- All employees are responsible for compliance with the Data Protection Policy and associated procedures at all times
- Employees should report any potential, actual or perceived data breaches to their line manager who will review and escalate when and where necessary and should follow the data breach process (to report potential / actual breaches)
- Ensure any required remediation for suspected or actual data breaches is resolved in a timely manner
- Complete all relevant Data Protection training and awareness including mandatory sight of relevant policies

Management Team

- Managers are responsible for ensuring adherence to this policy and associated procedures and processes within their areas of accountability
- Ensuring and monitoring that working practices within their areas of responsibility are compliant with all data protection regulations
- Establishing and maintaining documented procedures to ensure that anyone requesting confidential or personal data either in person, electronically or by telephone is appropriately authenticated before disclosing information
- Establishing and maintaining documented procedures to ensure personal data relating to customers is kept accurate and up to date

Second Line of audit

The Governors, supported by the DPO, are responsible for ensuring; -

- Company registration with the ICO is maintained
- Ensuring that company policies and standards & controls are adequately defined and implemented to ensure compliance with all Data Protection Regulations
- Challenge and ensure oversight of first line procedures to ensure compliance with all the requirements of this policy and associated standards and controls
- Providing clarification and guidance on any aspect of compliance with all data protection regulations.

If you observe a breach of this Policy, please speak to your line manager or the DPO.

Any failure to comply with this Policy may constitute a disciplinary matter for the person concerned and, in some cases, they could also incur employment or personal liability (where applicable).

For any clarification, please refer to your Line Manager, DPO or Headteacher.

Definitions

Controller	The company who process Personal Data.
DP Legislation	All relevant data protection legislation, ICO codes of practice and guidance which applies to the company and includes the Data Protection Act 2018, the General Data Protection Regulation, the Privacy and Electronic Communications Regulations 2003 and the Directive on Privacy and Electronic Communications (the ePrivacy Directive).
Data Subject	An individual who is the subject of any Personal Data.
DPIA	Data Privacy Impact Assessment
Data Protection Officer (DPO)	The individual within the company who has oversight for data protection compliance.
GDPR	The General Data Protection Regulation which is adopted in the UK through the Data Protect Act 2018.
ICO	The Information Commissioner's Office who are the UK regulator that is responsible for the oversight and enforcement of Data Protection legislation.
Personal Data	Data relating to a living individual.
Policy	The Data Protection Policy.