Egerton Rothesay School

Data Protection Policy

1. Compliance

This policy meets the requirements of the General Data Protection Regulation (GDPR), the Data Protection Act 2018, and is based on guidance published by the Information Commissioner's Office and the Department for Education

2. About this Policy

Egerton Rothesay School processes personal information relating to pupils, staff, parents and visitors and is, therefore, a Data Controller.

The school is registered as a Data Controller with the Information Commissioner's Office and renews this registration annually. The school's registration number is Z4609205

This policy sets out the obligations of Egerton Rothesay School regarding data protection and the rights of staff, pupils and parents in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation (GDPR).

During the course of its activities the school will process personal data (which may be held on paper, electronically or otherwise) about the school's staff (including temporary and agency staff), volunteers, pupils, their parents, guardians or carers, and other individuals (including suppliers and directors/governors).

The purpose of this policy is to make individuals (referred to as 'data subjects' under data protection law) aware of how the school will handle personal data of pupils, parents, guardians, staff and other individuals.

3. Roles and Responsibilities

Egerton Rothesay School Ltd has overall responsibility for policies and procedures relating to data protection and for ensuring compliance with the GDPR. The Board of Directors for Egerton Rothesay School Ltd have delegated responsibility for overseeing and monitoring the school's data protection procedures and to ensure their compliance with the GDPR to the school's Data Protection Officer (DPO).

The Data Protection Officer, working with the Leadership Group and Board of Directors, will be responsible for overseeing the implementation of this policy and for monitoring compliance with this policy, the school's other data protection related policies and with the GDPR and other applicable data protection legislation

The school's Data Protection Officer is Mrs Cherry Martin. Mrs Martin can be contacted by email at dpo@eger-roth.co.uk

All staff receive training in data protection and the General Data Protection Regulation and are responsible for ensuring that they collect, store and use any personal data in accordance with this policy.

4. Definitions

The table below provides definitions of terms used in this policy

Term	Definition
Personal Data	Data from which a person can be identified, including data that, when combined with other readily available information, leads to a person being identified
Special categories of personal data (formerly sensitive data)	Data such as • Racial or ethnic origin • Political opinions • Religious beliefs, or beliefs of a similar nature • Where a person is a member of a trade union • Physical and mental health • Sexual orientation • Biometric or genetic data Data relating to criminal offences is also afforded similar special protection
Processing	Processing covers a wide range of operations performed on personal data by manual or automated means. It includes the collection, recording, organisation, storage, adaptation/alteration, retrieval, consultation, use, disclosure, making available, restriction, erasure or destruction of personal data.
Data subject	The person whose personal data is held or processed
Data Controller	A person or organisation that determines the purpose for which, and the manner in which, personal data is processed
Processor	A person or organisation that processes personal data on behalf of a Controller

5. The Data Protection Principles

Egerton Rothesay School will comply with the principles set out in the GDPR, which require that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving or statistical purposes shall not be considered to be incompatible with the initial purposes

- Adequate, relevant and limited to what is necessary in relation to the purpose for which it is maintained
- Accurate and, where necessary, kept up to date. Every reasonable step will be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay
- 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
- Processed in a manner that ensures appropriate security of the personal data

Fair, Lawful and Transparent Data Processing

The school will only process personal data where it is based on one or more of the conditions specified in the GDPR. The conditions the school most commonly relies on to process personal data are as follows:

Conditions for processing data
Personal Data
• The data subject has given consent to the processing for one or more specific purposes • Processing is necessary for entering or performing a contract with the data subject • Processing is necessary for compliance with a legal obligation to which the data controller is subject • Processing is necessary in order for the data controller to perform a task carried out in the public interest or in the exercise of official authority vested in the data controller • Processing is necessary for the purposes of legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the subject is a child
Special Category Data
• The data subject has given explicit consent to the processing for one or more specific purposes • Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security and social protection law (insofar as it is authorised by EU or EU Member State law or a collective agreement pursuant to EU Member State law which provides appropriate safeguards for the fundamental rights and interests of the data subject) • Processing is necessary to protect the vital interests of the data subject or of another natural person, where the data subject is physically or legally incapable of giving consent • Processing relates to personal data which is clearly made public by the data subject • Processing is necessary for reasons of substantial public interest • Processing is necessary for the establishment, exercise or defence of legal claims Processing is necessary for the purposes of preventative or occupational medicine,

	for assessment of the working capacity of an employee, for medical diagnosis, for provision of health or social care or treatment, or the management of health or social care systems and services on the basis of EU or EU Member State law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the GDPR

The full list of conditions is set out in Articles 6 and 9 of the GDPR and the school may in some circumstances rely on other conditions set out in the GDPR or Data Protection Act 2018 to justify the processing of personal data or special category personal data. Further information about the lawful conditions for processing can also be found on the website of the Information Commissioner's Office

How and why the school processes personal data

The school routinely processes personal data about individuals, including current, past and prospective pupils, their parents and employees. This data includes the following:

- Contact details including addresses, telephone numbers and email addresses
- Financial information including bank details e.g. in respect of fee payment by parents and payroll details for staff
- Past, present and prospective pupils' educational records, including information about special educational needs
- Where appropriate, information about the physical and/or mental health of individuals
- Information and references provided by the school or received from other educational settings, organisations or professionals about pupils or staff
- Images of pupils and other individuals engaging in school activities and images captured by the school's CCTV cameras, in accordance with the school's policy on taking and using images of children

The school may process special category personal data relating to pupils and prospective pupils, including as appropriate:

- Information about a pupil's physical or mental health or condition (including but not limited to allergies and regular medications) in order to discharge the school's duty of care, provide non-emergency and emergency medical assistance and for special educational needs provision
- Information relating to provision for pupils with an Education, Health and Care Plan/Statement of Special Educational Needs
- The pupil's racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation or to ensure that religious or similar beliefs are respected
- In order to comply with other legal requirements and obligations to third parties

It is unlikely that school will process special category personal data relating to parents, guardians, carers and other individuals. However, where this may be necessary, it may include as appropriate:

- Information about racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation
- Relevant medical information needed for health and safety purposes
- In order to comply with other legal requirements and obligations to third parties

The school uses personal data about individuals for a number of purposes, including as follows:

- To support pupil learning
- To safeguard children and young people
- To provide appropriate pastoral care and support
- To monitor and report on pupil progress
- To enter pupils for external examinations/qualifications and to apply for Access Arrangements
- To support the selection of pupils as part of the admissions process
- To support decisions about what to do after leaving school
- To provide information to other educational settings attended after leaving ERS
- To support or improve educational provision
- For staff recruitment including statutory safeguarding checks
- In relation to the payment of school fees
- To comply with the law regarding data sharing
- Where otherwise reasonably necessary for the school's purposes, including to obtain appropriate professional advice and insurance for the school

Processing for specified, explicit and legitimate purposes

The school will only process personal data for the specific, explicit and legitimate purpose or purposes notified to data subjects. Personal data will not be further processed in any manner incompatible with that purpose unless the data subject has been informed of the new purpose and have given their consent where necessary.

Adequate, relevant and limited to what is necessary

Personal data will only be processed to the extent that it is relevant and necessary for the specific purposes of which the data subject has been notified.

Staff will only process data when their role requires it and will not process personal data for any reason unrelated to their role.

Accurate and, when necessary, kept up to date

Personal data held by the school will be kept accurate and, when necessary, up to date. Data that is inaccurate or out of date will be corrected or deleted without delay. Data subjects should notify the school if any personal detail changes or if the data subject becomes aware of any inaccuracies in the personal data held about him/her.

Data Retention

The school will not keep personal data for longer than is necessary for the purpose for which it is held, unless required by law to retain the information for a specified period of time.

Staff will take all reasonable steps to destroy or delete personal data that they hold when it is no longer required in accordance with the school's Data Retention Policy

Data Security

The school will ensure that appropriate measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Appropriate measures include:

- Appropriate levels of authority given to staff members where access to personal information is required
- Personal information processed only for authorised purposes
- Individuals who are not school staff may only access personal data with specific authority or consent
- Personal data is stored on in-house servers, maintained by the school IT team and remotely backed up offsite
- Computers and laptops are not left unattended without locking screens via password controls to prevent unauthorised access
- Personal data may only be accessed remotely on a secure device and for an authorised purpose.
- Personal data may only be taken off site for an authorised purpose on a password protected laptop or encrypted memory stick
- Personal data held on paper may only be used offsite for a specific, identified purpose, with the permission of the Headteacher or a member of the school leadership team
- Personal data held on paper is stored in lockable cabinets, drawers and cupboards
- All devices used for ERS business must be secure and password protected

6. Sharing information with third parties

The school has in place policies and procedures to maintain the security of all personal data from the point of collection to the point of destruction. The school will only transfer personal data to a third party where the third party agrees to comply with those policies and procedures.

Where the school uses a third party processor to process personal data on its behalf, it will have in place a written agreement with each processor which meets the requirements of Article 28 of the GDPR.

The school routinely shares information with:

- Schools/settings the pupil attends after leaving ERS
- The local authority of pupils who have an Education, Health and Care Plan (EHCP)
- The Department for Education (DfE)
- The National Health Service (NHS)
- Awarding Bodies (for qualifications/examinations)

- Joint Council for Qualifications
- Independent Schools Inspectorate (ISI), Independent Schools Association (ISA)

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

The school will share information when necessary with multiple agencies involved in forming a team around the child/young person. These agencies will be data controllers and are subject to the same obligations under data protection law as the school.

The school is required by law to provide information about our pupils to the DfE as part of statutory data collections, such as the school census; some of which information is then stored in the National Pupil Database (NPD).

The school will share pupil information with the ISI and ISA in respect of school inspection and/or registration

7. Transferring data outside the European Economic Area (EEA)

The school will only transfer any personal data it holds to a country outside the EEA if one of the following conditions applies:

- The country ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data as determined by the European Commission or where the organisation receiving the data has provided adequate safeguards
- The data subject has provided explicit consent
- The transfer is necessary for one of the conditions set out in the GDPR
- The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims
- The transfer is authorised by the Information Commissioner where we have adduced adequate safeguards with respect to the protection of the data subject's privacy, their fundamental rights and freedoms and the exercise of their rights

8. Subject Access Rights

Data subjects have the following rights:

Keeping data subjects informed

- This policy and accompanying privacy notices set out information about how the school processes personal data about pupils, parents and others. It will be reviewed annually to ensure transparency about processing of personal data

Data Subject Access

- Data subjects may make subject access requests (SARs) at any time to find out more about the personal data which the school holds about them, how it is processing that data and why
- Under data protection laws, pupils over 12 years of age have a right to request access to the information the school holds about them. If the pupil is unable to

understand their rights and the implications of a subject access request, or has given their consent, their parent may make a subject access request

- Subject access requests must be submitted in writing, either by letter or email, to the school's Data Protection Officer (DPO), Mrs Cherry Martin dpo@eger-roth.co.uk
- Requests should include the data subject's name, contact details and details about information being requested

The school will not reveal the following information in response to subject access requests

- Information that might cause serious harm to the physical or mental health of the pupil or another individual
- Information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests
- Information contained in adoption and parental order records

Rectification of personal data

- Data subjects have the right to request the school to rectify any inaccuracies in personal data processed by the school

Erasure of personal data

- If the school has no compelling reason to process data about an individual, they have the right to have the data erased and processed no further. This is not an absolute right and the school will consider requests on a case by case basis

Restriction of personal data processing

- Processing of personal data can be restricted whilst the school considers if any personal data is inaccurate or if an objection has been raised about the data that is being processed

Data portability

- Where a data subject has given their consent for personal data to be processed using automated means, they have the right to receive a copy of that personal data in order to use it for other purposes (namely to transmit to a third party)
- Where technically feasible, if requested by the data subject, personal data will be sent directly to the required third party

Objection to data processing

- Data subjects have the right to object to the processing of personal data for the performance of a task in the public interest or based on legitimate interests
- The school will consider any objection but may be able to demonstrate legitimate grounds for continuing to process the personal data concerned

Automated decision making and profiling

- The school will inform data subjects of any automated decision making processes it uses. Data subjects are entitled to request that automated decisions involving them are reviewed by human intervention

9. Data Breach Notification

All personal data breaches must be reported to the Data Protection Officer

If a personal data breach occurs that is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage) the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay.

In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without delay

If you have a concern about the way Egerton Rothesay School is collecting or using your personal data, you can raise your concern with the Information Commissioner's Office (ICO). The ICO can be contacted from Monday to Friday (9am – 5pm) on 0303 123 1113

Policy approved by: Alison Walker
(on behalf of Governing Body)
Date:24.09.20
Next Review(latest) September 2021

Appendix 1: Working from Home: Guidance for Staff

All staff are responsible for ensuring that any data they use is adequately protected and that no-one else has access to school data they are using when working from home. Staff must adhere to the following guidelines in conjunction with existing data protection and retention policies.

Use of approved technology for handling personal data

If you have been provided with any technology by ERS (hardware or software), you should use this. This will provide the best protection for personal data.

You must avoid the temptation to do things in a way you might find more convenient, such as sending emails through a personal account or using the video conferencing app that you use with friends for work calls.

Confidentiality when holding conversations or using a screen

If you share your home working space with other family members or friends, you should endeavour to hold conversations, where they are less likely to be overheard and screens should be positioned where they are less likely to be overseen.

If you are using a home or shared device, or sharing a work space, you must log out of emails, Staffweb and other school related programmes when you are not using them. Passwords should not be saved on any device which others can access.

Taking care with print outs

All confidential waste must be shredded or stored securely until it can be disposed of securely in school.

Keeping data and devices secure

If you have to work using your own device and software, ERS data must be kept separate to avoid accidentally keeping hold of data for longer than is necessary.

You must remove all data from your devices when it is no longer needed or at school's request. You should also regularly check that all ERS related data is cleared from downloads on your device.

To avoid loss or theft of personal data, print outs and devices should be put away at the end of the working day. Personal data must not be left where it can be read by others.

Opening web links and attachments in emails or other messages

Do not not click on unfamiliar web links or attachments and follow the National Cyber Security Centre's (NCSC) guidance on spotting suspicious emails.

Use of strong passwords

Whether using online storage, a laptop or some other technology, it's important that you make passwords hard to guess. The NCSC recommends using three random words together as a password (eg 'coffeetrainfish' or 'walltincake'). Make sure you use different passwords for different services too.

Communicating securely

Use the communication facilities provided by ERS whenever possible If you need to share data with others you should use online secure systems where available or school email accounts. If email is used, you should consider whether it is necessary to password protect* the document.

Keeping software up to date

If you are using your own equipment, you must keep your device fully up to date with anti-virus, malware and security updates. If you have an ERS laptop it will automatically back up and update when you next come in to school and log on to the network.

Use of Wi-Fi

If you are using your own WI-FI it must be password protected. You should not use public or shared Wi-Fi for accessing and sharing ERS data

Data breaches

You must report ALL data breaches to Cherry Martin (DPO) immediately.

***How to protect a document with a password**

Passwords are case-sensitive and can be a maximum of 15 characters long.

If you lose or forget your password, Word won't be able to recover it for you. Be sure to keep a copy of the password in a safe place or create a strong password that you'll remember.

1. Go to **File** > **Info** > **Protect Document** > **Encrypt with Password**.
2. Type a password, then type it again to confirm it.
3. Save the file to make sure the password takes effect.