UK General Data Protection Regulation (GDPR) Policy

Written by	Adopted by Governing Body	Review Date
Jade Driscoll – Autumn Term 2020	January 2021	June 2025
Nicolien Lawson - review June 2025		June 2028

Summary of Key Changes June 2025

Section	Change Summary
Legal Framework	Replaced references to EU GDPR with UK GDPR post-Brexit, clarified legal references
DPO Role	Clarified that DPO must have no conflict of interest; must meet independence standards under UK GDPR
Consent & Children	Updated age of digital consent (13 in UK) and clarified rules around counselling services
Data Security	Strengthened language on multi-factor authentication, removal of USB memory sticks, use of cloud-based services
Data Breaches	Included updated reporting requirements under UK GDPR and ICO guidance
Retention & Review	Emphasised compliance with the IRMS toolkit for schools (2023) and review every 2 years or upon significant legal change
Automated Decision Making	Reframed with updated UK stance and referenced AI-related processing reviews
Terminology	General consistency improvements (e.g. using "UK GDPR", "data subjects", "DPO", etc.)

Contents

Statement of Intent

Riverview FoS is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the UK General Data Protection Regulation (UK GDPR).

The organisation may, from time to time, be required to share personal information about its staff or students with other organisations, mainly the Local Authority (LA), other schools/academies and educational bodies, social services and other organisations who provide services to us.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the Riverview FoS complies with the following core principles of UK GDPR.

This policy complies with the requirements set out in the UK GDPR, which came into effect on 25 May 2018.

1 Legal Framework

This policy has due regard to relevant UK data protection legislation, including but not limited to the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

This policy will be implemented in conjunction with the following other policies:

- Data & Document Retention Policy
- IT Policy and Acceptable Use Policy
- Staff Code of Conduct
- AI Policy
- CCTV Policy

2 Scope

For the purpose of this policy, **personal data** refers to information that relates to an identifiable, living individual, including information such as an online identifier, such as an Internet Protocol (IP) address. The UK GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria.

Sensitive personal data is referred to in the UK GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data and data concerning health matters.

3 Principles

In accordance with the requirements outlined in the UK GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- 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.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- 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.
- 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 UK GDPR in order to safeguard the rights and freedoms of individuals.

- 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.

The UK GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

4 Accountability

Riverview FoS has implemented appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the UK GDPR.

Riverview FoS maintains comprehensive records of processing activities and conducts Data Protection Impact Assessments (DPIAs) where appropriate

5 Data Protection Officer (DPO)

The DPO at the Riverview FoS ensures compliance with the UK GDPR. The DPO must act independently, have no conflicts of interest, and report directly to the Federation Lead and Governors.

The DPO has professional experience and knowledge of data protection law, particularly that in relation to education.

The DPO ensures UK GDPR compliance, acts independently, advises the organisation and employees on their obligations, monitors compliance (including DPIAs and internal audits), provides mandatory training, and serves as the primary contact point for the Information Commissioner's Office (ICO).

The DPO will operate independently and will not be penalised for performing their task. Sufficient resources will be provided to the DPO to enable them to meet their UK GDPR obligations.

6 Lawful Bases for Processing Personal Data

The lawful basis for processing data will be identified and documented prior to data being processed. Under the UK GDPR, data will be lawfully processed under the following conditions:

Legal Basis

- Consent; the individual has given clear consent for you to process their personal data for a specific purpose;
- Contract; the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract
- Legal Obligation; the processing is necessary for you to comply with the law (not including contractual obligations)
- Vital Interests; the processing is necessary to protect someone's life

- Public task the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law
- Legitimate Interest: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

At least one of these must apply whenever personal data is processed.

Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by the 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 UK 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 sevices
    - 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).
    - A contract with a health professional.

7 Consent

Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

Where consent is given, a record will be kept documenting how and when consent was given. The Riverview FoS ensures that consent mechanisms meet the standards of the UK GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

Consent accepted under the DPA will be reviewed to ensure it meets the standards of the UK GDPR; however, acceptable consent obtained under the DPA will not be reobtained. Consent can be withdrawn by the individual at any time.

Under the **UK GDPR**, children aged **13 or over** can consent to online services (except where services relate to counselling). This also includes consenting to the use of their photographs for internal or external use, and the (withholding of) consent to the provision of data from a Subject Access Request (SAR) made by parents about the child.

8 The Right to be Informed

The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge, and can be accessed on the Riverview FoS website.

In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller, and where applicable, the controller's representative and the DPO.
- The purpose of, and the legal basis for, processing the data.
- The legitimate interests of the controller or third party.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to third parties and the safeguards in place.
- The retention period and the criteria used to determine the retention period.
- The existence of the data subject's rights, including the right to:
    - Withdraw consent at any time.
    - Lodge a complaint with a supervisory authority.
- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement and the details of the categories of personal data, as well as any possible consequences of failing to provide the personal data, will be provided.

Where data is not obtained directly from the data subject, information regarding the source the personal data originates from and whether it came from publicly accessible sources, will be provided.

For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

In relation to data that is not obtained directly from the data subject, this information will be supplied:

- Within one month of having obtained the data.
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
- If the data are used to communicate with the individual, at the latest, when the first communication takes place.

Privacy notices will be reviewed annually to ensure they remain accurate and up to date.

9 The Right of Access

Individuals have the right to obtain confirmation that their data is being processed.

Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing. the Riverview FoS will verify the identity of the person making the request before any information is supplied.

A copy of the information will be supplied digitally to the individual free of charge; however, the Riverview FoS may impose a 'reasonable fee' to comply with requests for further copies of the same information.

Requests will be responded to without delay and at the latest, within one month of receipt.

In the event of numerous or complex requests, the period of compliance may be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

In the event that a large quantity of information is being processed about an individual, the Riverview FoS will ask the individual to specify the information the request is in relation to. Where a SAR is deemed complex - such as those involving all emails and notes about a person - the response may be extended to three months in line with ICO guidance. This will be assessed on a case-by-case basis.

Where a request is manifestly unfounded or excessive or vexatious, the Riverview FoS holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the ICO within one month of the refusal.

If a SAR is from a parent about their child, and the child is 13 or over, then consent from the child will be sought first.

10 The Right to Rectification

Individuals are entitled to have any inaccurate or incomplete personal data rectified. Where the personal data in question has been disclosed to third parties, the Riverview FoS will inform them of the rectification where possible or necessary.

Where appropriate, the Riverview FoS will inform the individual about the third parties that the data has been disclosed to. Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

Where no action is being taken in response to a request for rectification, the Riverview FoS will explain the reason for this to the individual, and will inform them of their right to complain to the ICO.

11 The Right to Erasure

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.
Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

the Riverview FoS has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

Where personal data has been made public within an online environment, the Riverview FoS will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

12 The Right to Restrict Processing

Individuals have the right to block or suppress the Riverview FoS's processing of personal data.
In the event that processing is restricted, the Riverview FoS will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.
the Riverview FoS will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the Riverview FoS has verified the accuracy of the data
- Where an individual has objected to the processing and the Riverview FoS is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restrictions instead
- Where the Riverview FoS no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

If the personal data in question has been disclosed to third parties, the Riverview FoS will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.
the Riverview FoS will inform individuals when a restriction on processing has been lifted.

13 The Right to Data Portability

Individuals have the right to obtain and reuse their personal data for their own purposes across different services.
Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

Personal data will be provided in a structured, commonly used and machine-readable form. the Riverview FoS will provide the information free of charge.

Where feasible, data will be transmitted directly to another organisation at the request of the individual.

Riverview FoS is not required to adopt or maintain processing systems which are technically compatible with other organisations.

In the event that the personal data concerns more than one individual, the Riverview FoS will consider whether providing the information would prejudice the rights of any other individual. the Riverview FoS will respond to any requests for portability within one month.

Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

Where no action is being taken in response to a request, the Riverview FoS will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the Supervisory Authority and to a judicial remedy.

14 The Right to Object

This information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.
Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Processing for purposes of scientific or historical research and statistics.
- Where personal data is processed for the performance of a legal task or legitimate interests:
- An individual's grounds for objecting must relate to his or her particular situation.
- the Riverview FoS will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the Riverview FoS can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.
- Where personal data is processed for direct marketing purposes:
- the Riverview FoS will stop processing personal data for direct marketing purposes as soon as an objection is received.
- the Riverview FoS cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.
- Where personal data is processed for research purposes:
- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the Riverview FoS is not required to comply with an objection to the processing of the data.

Where the processing activity is outlined above, but is carried out online, the Riverview FoS will offer a method for individuals to object online.

15 The Right Not to be Subject to Automated Decision-Making

Individuals have the right to object to automated decision making. At the moment the Riverview FoS has not identified any processes where automated decision making is used but will keep this under review.

16 Privacy by Design and Privacy Impact Assessments

The Riverview FoS will act in accordance with the UK GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the

Riverview FoS has considered and integrated data protection into processing activities.

Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the Riverview FoS's data protection obligations and meeting individuals' expectations of privacy.

DPIAs will allow the Riverview FoS to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to Riverview FoS's reputation which might otherwise occur.

A DPIA will be used when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

A DPIA will be used for more than one project, where necessary.

High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences

The Riverview FoS will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk
- Use of AI
- Systematic monitoring
- Processing on a large scale of special category or criminal offence data

Where a DPIA indicates high risk data processing, the Riverview FoS will consult the Information Commissioner's Office (ICO) to seek its opinion as to whether the processing operation complies with the UK GDPR.

17 Data Breaches

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. All breaches are logged by the DPO.

The Federation Lead, along with the DPO, will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their continuous development training.

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the ICO will be informed. All notifiable breaches will be reported to the ICO within 72 hours of the Riverview FoS becoming aware of it.

The risk of the breach having a detrimental effect on the individual, and the need to notify the ICO, will be assessed on a case-by-case basis. In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the Riverview FoS will notify those concerned directly.

A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the ICO. In the event that a breach is sufficiently serious, the public will be notified without undue delay, using clear and plain language."

Effective and robust breach detection, investigation and internal reporting procedures are in place,

which facilitate decision-making in relation to whether the ICO or the public need to be notified.

Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

18 Data Security

Riverview FoS will apply the following measures at all times:

- Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.
- Confidential paper records will not be left unattended or in clear view anywhere with general access.
- Digital data is coded, encrypted or password-protected, on a network drive that is regularly backed up off-site.
- Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.
- Permissions will be controlled to ensure that only the appropriate people have access to data on Arbor/Google Drive and other systems
- Memory sticks will not be used in school. Staff must use encrypted cloud-based storage provided by the Riverview FoS.
- All electronic devices are password-protected to protect the information on the device in case of theft. Stolen or missing devices are reported immediately.
- The Riverview FoS enables electronic devices to allow the remote blocking or deletion of data in case of theft.
- Staff and Governors are permitted to use personal devices for school purposes but must ensure that appropriate software is used. Passwords must not be shared with anyone else and particular regard should be made if other family members use the device to ensure they cannot access personal /school data.
- All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password. Staff must ensure that 2 Factor Authentication is enabled and in use.
- Personal sensitive or confidential information should not be sent by email unless encrypted and password-protected
- All email communication to parents should be via the approved communications systems: Arbor and Gmail.
- Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the premises accepts full responsibility for the security of the data.
- Before sharing data, all staff members will ensure:
    - They are authorised to share it in accordance with the school's policies and lawful basis under UK GDPR.
    - That adequate security is in place to protect it.
    - Who will receive the data has been outlined in a privacy notice.
- Under no circumstances are visitors allowed access to confidential or personal information.
- Visitors to areas of the organisation containing sensitive information are supervised at all times.
- The physical security of the buildings and storage systems, and access to them, is reviewed on a **termly** basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

Riverview FoS takes its duties under the UK GDPR seriously and any unauthorised disclosure may

result in disciplinary action.

The Data Protection Officer is responsible for continuity and recovery measures are in place to ensure the security of protected data.

19 Publication of Information

Riverview FoS will not publish any personal information, including photos, on its website or social media without the permission of the affected individual.

20 Closed Circuit Television and Photography

The Riverview FoS understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

Please read the Riverview FoS CCTV Policy in conjunction with this document.

21 Data Retention

Data will not be kept for longer than is necessary in line with the Riverview FoS Data and Document Retention Policy. the Riverview FoS will adopt guidance from the IRMS Toolkit for Schools (2023). Reviews will occur at least biennially or when major legal updates are issued.

Some educational records relating to former pupils or employees of the Riverview FoS may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

22 Disclosure and Barring Service (DBS) Data

All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

Data provided by the DBS will never be duplicated.

Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

23 Policy Review

This policy is reviewed by the Data Protection Officer and the Head Teacher, as per the schedule at the start of this document.

Signed (Chair)		**Signed (Head)**	
Date		**Date**	