Data Protection Policy

The Rivers C of E Academy Trust

Committee:	Audit, Risk and Compliance Committee
Approved on:	July 2025
Next review date:	July 2026

Requirements for Publication

Section of the Policy	Notes and Clarity of Definitions
Notifications throughout on Headteacher responsibilities	For Head of Schools, please refer to your Executive Head for guidance and support

Data Protection Policy

Contents

1 Policy statement

1.1 Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities as Rivers C of E Academy Trust we will collect, store and process personal data about our pupils, workforce, parents and others. This makes us a data controller in relation to that personal data.

1.2 We are committed to the protection of all personal data and special category personal data for which we are the data controller.

1.3 The Trust processes personal data in accordance with all requirements of UK Data Protection legislation, including the UK GDPR, the Data Protection Act 2018, and the Data (Use and Access) Act 2025.

1.4 The law imposes significant fines for failing to lawfully process and safeguard personal data and failure to comply with this policy may result in those fines being applied.

1.5 All members of our workforce must comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary or other action.

1.6 This policy has been approved by the Board of Trustees of The Rivers C of E Academy Trust and takes into account the values and ethos we hold as a trust. Staff and pupils are under no obligation to disclose to the Trust their race or ethnic origin, political or religious beliefs.

2 About this policy

2.1 The types of personal data that we may be required to handle include information about pupils, parents, our workforce, and others that we deal with. The personal data which we hold is subject to certain legal safeguards specified in the General Data Protection Regulation ('GDPR'), the [Data Protection Act 2018], and other regulations including the Data (Use and Access) Act 2025

2.2 This policy and any other documents referred to in it, set out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

2.3 This policy does not form part of any employee's contract of employment and may be amended at any time.

2.4 This policy sets out rules on data protection and the legal conditions that must be satisfied when we process personal data.

3 Definition of data protection terms

3.1 All defined terms in this policy are indicated in bold text, and a list of definitions is included in the Annex to this policy.

4 Data Protection Officer

4.1 As Rivers C of E Academy Trust, we are required to appoint a Data Protection Officer ("DPO"). Our DPO is Fyonna Lammas, she can be contacted at dpo@riverscofe.co.uk.

4.2 The DPO is responsible for ensuring compliance with the Data Protection Legislation and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPO.

4.3 The DPO is also the central point of contact for all data subjects and others in relation to matters of data protection.

5 Data protection principles

5.1 Anyone processing personal data must comply with the data protection principles. These provide that personal data must be:

5.1.1 Processed fairly and lawfully and transparently in relation to the data subject;

5.1.2 Processed for specified, lawful purposes and in a way which is not incompatible with those purposes;

5.1.3 Adequate, relevant and not excessive for the purpose;

5.1.4 Accurate and up to date;

5.1.5 Not kept for any longer than is necessary for the purpose; and

5.1.6 Processed securely using appropriate technical and organisational measures.

5.2 Personal Data must also:

5.2.1 be processed in line with data subjects' rights;

5.2.2 not be transferred to people or organisations situated in other countries without adequate protection.

5.3 We will comply with these principles in relation to any processing of personal data by our schools or trust.

6 Fair and lawful processing

6.1 Data Protection Legislation is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

6.2 For personal data to be processed fairly, data subjects must be made aware:

6.2.1 that the personal data is being processed;

6.2.2 why the personal data is being processed;

6.2.3 what the lawful basis is for that processing (see below);

6.2.4 whether the personal data will be shared, and if so with whom;

6.2.5 the period for which the personal data will be held;

6.2.6 the existence of the data subject's rights in relation to the processing of that personal data; and

6.2.7 the right of the data subject to raise a complaint with the Information Commissioner's Office in relation to any processing.

6.3 We will only obtain such personal data as is necessary and relevant to the purpose for which it was gathered, and will ensure that we have a lawful basis for any processing.

6.4 For personal data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in the Data Protection Legislation. We will normally process personal data under the following legal grounds:

6.4.1 where the processing is necessary for the performance of a contract between us and the data subject, such as an employment contract;

6.4.2 where the processing is necessary to comply with a legal obligation that we are subject to, (e.g. the Education Act 2011);

6.4.3 where the law otherwise allows us to process the personal data or we are carrying out a task in the public interest; and

6.4.4 where none of the above apply then we will seek the consent of the data subject to the processing of their personal data.

6.4.5 Where the processing is permitted under the Data (Use and Access) Act 2025 for public service delivery, safeguarding, or fraud prevention, provided appropriate safeguards are in place.

6.5 When special category personal data is being processed then an additional legal ground must apply to that processing. We will normally only process special category personal data under following legal grounds:

6.5.1 where the processing is necessary for employment law purposes, for example in relation to sickness absence;

6.5.2 where the processing is necessary for reasons of substantial public interest, for example for the purposes of equality of

opportunity and treatment;

6.5.3 where the processing is necessary for health or social care purposes, for example in relation to pupils with medical conditions or disabilities; and

6.5.4 where none of the above apply then we will seek the consent of the data subject to the processing of their special category personal data.

6.6 We will inform data subjects of the above matters by way of appropriate privacy notices which shall be provided to them when we collect the data or as soon as possible thereafter, unless we have already provided this information such as at the time when a pupil joins us.

6.7 If any data user is in doubt as to whether they can use any personal data for any purpose then they must contact the DPO before doing so.

Vital Interests

6.8 There may be circumstances where it is considered necessary to process personal data or special category personal data in order to protect the vital interests of a data subject. This might include medical emergencies where the data subject is not in a position to give consent to the processing. We believe that this will only occur in very specific and limited circumstances. In such circumstances we would usually seek to consult with the DPO in advance, although there may be emergency situations where this does not occur.

Consent

6.9 Where none of the other bases for processing set out above apply then the school must seek the consent of the data subject before processing any personal data for any purpose.

6.10 There are strict legal requirements in relation to the form of consent that must be obtained from data subjects.

6.11 When pupils and or our Workforce join the Rivers C of E Academy Trust a consent form will be required to be completed in relation to them. This consent form deals with the taking and use of photographs and videos of them, amongst other things. Where appropriate third parties may also be required to complete a consent form.

6.12 In relation to all pupils under the age of 12/13 years old we will seek consent from an individual with parental responsibility for that pupil.

6.13 We will generally seek consent directly from a pupil who has reached the age of 12/13, however we recognise that this may not be appropriate in certain circumstances and therefore may be required to seek consent from and individual with parental responsibility.

6.14 If consent is required for any other processing of personal data of any

data subject then the form of this consent must:

6.14.1 Inform the data subject of exactly what we intend to do with their personal data;

6.14.2 Require them to positively confirm that they consent – we cannot ask them to opt-out rather than opt-in; and

6.14.3 Inform the data subject of how they can withdraw their consent.

6.15 Any consent must be freely given, which means that we cannot make the provision of any goods or services or other matter conditional on a data subject giving their consent.

6.16 The DPO must always be consulted in relation to any consent form before consent is obtained.

6.17 A record must always be kept of any consent, including how it was obtained and when.

7 Processing for limited purposes

7.1 In the course of our activities as a School and/or Trust, we may collect and process the personal data set out in our Schedule of Processing Activities. This may include personal data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and personal data we receive from other sources (including, for example, local authorities, other schools, parents, other pupils or members of our workforce).

7.2 We will only process personal data for the specific purposes set out in our Schedule of Processing Activities or for any other purposes specifically permitted by Data Protection Legislation or for which specific consent has been provided by the data subject.

8 Notifying data subjects

8.1 If we collect personal data directly from data subjects, we will inform them about:

8.1.1 our identity and contact details as Data Controller and those of the DPO;

8.1.2 the purpose or purposes and legal basis for which we intend to
process that personal data;

8.1.3 the types of third parties, if any, with which we will share or to which we will disclose that personal data;

8.1.4 whether the personal data will be transferred outside the European Economic Area ('EEA') and if so the safeguards in place;

8.1.5 the period for which their personal data will be stored, by reference to our Retention and Destruction Policy;

8.1.6 the existence of any automated decision making in the processing of the personal data along with the significance and envisaged consequences of the processing and the right to object to such decision making; and

8.1.7 the rights of the data subject to object to or limit processing, request information, request deletion of information or lodge a complaint with the ICO.

8.2 Unless we have already informed data subjects that we will be obtaining information about them from third parties (for example in our privacy notices), then if we receive personal data about a data subject from other sources, we will provide the data subject with the above information as soon as possible thereafter, informing them of where the personal data was obtained from.

9 Adequate, relevant and non-excessive processing

9.1 We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject, unless otherwise permitted by Data Protection Legislation.

10 Accurate data

10.1 We will ensure that personal data we hold is accurate and kept up to date.

10.2 We will take reasonable steps to destroy or amend inaccurate or out-of-date data. Data subjects have a right to have any inaccurate personal data rectified. See further below in relation to the exercise of this right.

11 Timely processing

11.1 We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all personal data which is no longer required.

12 Processing in line with data subject's rights

12.1 We will process all personal data in line with data subjects' rights, in particular their right to:

12.1.1 request access to any personal data we hold about them;

12.1.2 object to the processing of their personal data, including the right to object to direct marketing;

12.1.3 have inaccurate or incomplete personal data about them

rectified;

12.1.4 restrict processing of their personal data;

12.1.5 have personal data we hold about them erased

12.1.6 have their personal data transferred; and

12.1.7 object to the making of decisions about them by automated means.

12.1.8 In line with the Data (Use and Access) Act 2025, data subjects have the right to be informed if their data is accessed by public bodies under the lawful bases introduced in the Act. This includes the right to request details about how their data was accessed, for what purpose, and by whom, unless an exemption applies (e.g. for safeguarding, fraud prevention, or national security purposes).

The Right of Access to Personal Data

12.2 Data subjects may request access to all personal data we hold about them. Such requests will be considered in line with the Trust's Subject Access Request Procedure.

The Right to Object

12.3 In certain circumstances data subjects may object to us processing their personal data. This right may be exercised in relation to processing that we are undertaking on the basis of a legitimate interest or in pursuit of a statutory function or task carried out in the public interest.

12.4 An objection to processing does not have to be complied with where the school can demonstrate compelling legitimate grounds which override the rights of the data subject.

12.5 Such considerations are complex and must always be referred to the DPO upon receipt of the request to exercise this right.

12.6 In respect of direct marketing any objection to processing must be complied with.

12.7 The Rivers C of E Academy Trust is not however obliged to comply with a request where the personal data is required in relation to any claim or legal proceedings.

The Right to Rectification

12.8 If a data subject informs the Rivers C of E Academy Trust that personal data held about them by the Rivers C of E Academy Trust is inaccurate or incomplete then we will consider that request and provide a response within one month.

12.9 If we consider the issue to be too complex to resolve within that period then we may extend the response period by a further two months. If this is necessary then we will inform the data subject within one month of their request that this is the case.

12.10 We may determine that any changes proposed by the data subject should not be made. If this is the case then we will explain to the data subject why this is the case. In those circumstances we will inform the data subject of their right to complain to the Information Commissioner's Office at the time that we inform them of our decision in relation to their request.

The Right to Restrict Processing

12.11 Data subjects have a right to "block" or suppress the processing of personal data. This means that the Rivers C of E Academy Trust can continue to hold the personal data but not do anything else with it.

12.12 The Rivers C of E Academy Trust must restrict the processing of personal data:

12.12.1 Where it is in the process of considering a request for personal data to be rectified (see above);

12.12.2 Where the Rivers C of E Academy Trust is in the process of considering an objection to processing by a data subject;

12.12.3 Where the processing is unlawful but the data subject has asked the Rivers C of E Academy Trust not to delete the personal data; and

12.12.4 Where the Rivers C of E Academy Trust no longer needs the personal data but the data subject has asked the Rivers C of E Academy Trust not to delete the personal data because they need it in relation to a legal claim, including any potential claim against the School or Trust.

12.13 If the Rivers C of E Academy Trust has shared the relevant personal data with any other organisation then we will contact those organisations to inform them of any restriction, unless this proves impossible or involves a disproportionate effort.

12.14 The DPO must be consulted in relation to requests under this right.

The Right to Be Forgotten

12.15 Data subjects have a right to have personal data about them held by the Rivers C of E Academy Trust erased only in the following circumstances:

12.15.1 Where the personal data is no longer necessary for the purpose for which it was originally collected;

12.15.2 When a data subject withdraws consent – which will apply only where the Rivers C of E Academy Trust is relying on the individuals consent to the processing in the first place;

12.15.3 When a data subject objects to the processing and there is no overriding legitimate interest to continue that processing – see above in relation to the right to object;

12.15.4 Where the processing of the personal data is otherwise unlawful;

12.15.5 When it is necessary to erase the personal data to comply with a legal obligation; and

12.16 The Rivers C of E Academy Trust is not required to comply with a request by a data subject to erase their personal data if the processing is taking place:

12.16.1 To exercise the right of freedom of expression or information;

12.16.2 To comply with a legal obligation for the performance of a task in the public interest or in accordance with the law;

12.16.3 For public health purposes in the public interest;

12.16.4 For archiving purposes in the public interest, research or statistical purposes; or

12.16.5 In relation to a legal claim.

12.17 If the Rivers C of E Academy Trust has shared the relevant personal data with any other organisation then we will contact those organisations to inform them of any erasure, unless this proves impossible or involves a disproportionate effort.

12.18 The DPO must be consulted in relation to requests under this right.

Right to Data Portability

12.19 In limited circumstances a data subject has a right to receive their personal data in a machine readable format, and to have this transferred to other organisation.

12.20 If such a request is made then the DPO must be consulted.

13 Data security

13.1 We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

13.2 We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.

13.3 Security procedures include:

13.3.1 Entry controls. Any stranger seen in entry-controlled areas should be reported to Headteacher or appropriate line manager.

13.3.2 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.)

13.3.2 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 Information Commissioner's Office guidance on the disposal of IT assets.

13.3.3 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.

13.3.4 Working away from the school premises – paper documents. There should be a general presumption against taking paper records containing personal or other confidential data off-site and it should only happen when it is absolutely essential to do so and there is no alternative method for accessing or recording the information required, eg scanning or accessing online via an encrypted tablet. Where it is determined that it is a necessity to take paper records off-site, the following principles must be adopted and followed, to minimise the theft, loss or unauthorised use of personal or other confidential data whilst in transit or off- site:

(i) Only a minimum amount of data necessary for the job in hand should be removed;

(ii) When in transit from one location to another, records should be transported in a way that mitigates the risks of theft or loss, eg if it is unavoidable to leave paper records in a car they should be locked in the boot, records should not be stored in a car overnight, when travelling on public transport paper records should be kept close by at all times, paper records should not be carried 'loosely';

(iii) Whilst off-site, and/or temporarily in the home of a staff member, paper records containing personal or other confidential data that are not being actively worked on must be kept secure and separate from valuable items such as laptops.

(iv) Paper records taken out of the office should be returned to the place of work as soon as possible. They should not be kept out of the office for any longer than is necessary to complete the job in hand.

13.3.5 Working away from the school premises – electronic working.

(i) When working in any public environment care should be taken to ensure that no bystander could overlook any information displayed on the device or any user input (especially passwords). The security and confidentiality of data and equipment must be considered at all times.

(ii) Staff working remotely should do so via remote access to the Trust and/or school network or their Trust OneDrive account (ensuring synchronisation is switched off). Data must not be stored on USB data sticks, CDs, external hard drives, cameras or any other removable media storage device unless they have been given explicit permission by their Headteacher/Executive leader and the device has been appropriately encrypted.

(iii) Staff are prohibited from downloading information onto personal devices, Drop-box, iCloud or any other cloud storage not managed by the Trust and/or school.

(iv) Emails must not be diverted to a personal email address.

(v) When in transit from one location to another, electronic devices provided by the Trust and/or school, such as laptops, should be transported in a way that mitigates the risks of theft or loss, eg electronic devices should not be stored in a car overnight, when travelling on public transport electronic devices should be kept close by at all times.

(vi) Where electronic devices provided by the Trust and/or school are kept overnight they should be stored securely, out of sight.

13.3.6 Document printing. Documents containing personal data must be collected immediately from printers and not left on photocopiers.

13.3.7 The Rivers CofE Academy Trust adheres to a Trust-wide Retention and Destruction Schedule, which outlines how long different types of personal data must be retained and the secure disposal methods to be used. These retention periods are aligned with statutory guidance, legal requirements, and operational needs.

13.3.8 To ensure the safe and compliant destruction of personal data:

Confidential paper waste is collected and shredded by an

accredited third-party provider. Certificates of destruction are issued and retained as part of our audit trail.

IT assets (including laptops, hard drives, and USBs) are disposed of by a certified IT asset disposal company. Devices are wiped to industry standards and a data destruction certificate is issued for each item.

These processes are supported by internal data disposal procedures, which ensure that only authorised personnel carry out or arrange data destruction and that records are maintained in accordance with the Trust's information governance framework.

No data is disposed of informally or without due documentation. The DPO is responsible for ensuring these controls are maintained and audited periodically.

13.4 Any member of staff found to be in breach of the above security measures may be subject to disciplinary action.

14 Cyber Security

14.1 The Rivers CofE Academy adheres to the guidance from the Department for Education (DfE) Cyber Security Standards for Schools and Colleges, updated in May 2024. In partnership with our managed service provider, Joskos, we ensure that data and user information are securely stored. This includes the management of privileges, licenses, and backups to safeguard our digital resources, as outlined in our Cloud Computing Protocol and Acceptable Use Protocol.

14.2 In alignment with the principles of data protection by design and by default, and to ensure compliance with the UK GDPR and the Data (Use and Access) Act 2025, The Rivers CofE Academy Trust implements a robust set of cyber security controls. These measures are designed to protect the confidentiality, integrity, and availability of personal data held across the Trust. Current technical and organisational controls include:

14.3 Mandatory Multi-Factor Authentication (2FA) for all staff accounts to reduce the risk of unauthorised access

14.4 Regular cloud-based backups of critical systems and data to ensure recovery in the event of a data loss incident

14.5 Ongoing anti-phishing training and simulation campaigns for staff, alongside automatic filtering of suspicious emails

14.6 Microsoft Defender for Endpoint and other threat detection tools deployed across all Trust-managed devices

14.7 Regular penetration testing and vulnerability assessments carried out by our managed service provider (Joskos)

14.8 Encryption of devices and secure mobile device management policies, including remote wipe capability

14.9 24/7 monitoring and alerting for anomalies or potential breaches by our managed service partner

14.10 These controls are reviewed regularly in partnership with the Trust's IT provider to ensure they reflect the current threat landscape and best practice.

15 Data Protection Impact Assessments

15.1 The Rivers CofE Academy Trust takes data protection very seriously and will consider and comply with the requirements of Data Protection Legislation in relation to all of its activities whenever these involve the use of personal data, in accordance with the principles of data protection by design and default.

15.2 In certain circumstances we carry out detailed assessments of proposed processing. We do this through a Data Protection Impact Assessment (DPIA).

15.3 A Data Protection Impact Assessment (DPIA) should be carried out in the following cases:

- Systematic and extensive evaluation of personal aspects of an individual, including profiling.
- Processing of sensitive data on a large scale.
- Before commencing high-risk processing activities to assess data protection risks.
- At the early stages of a project or when significant changes are made to processing operations.

15.4 The DPO should always be consulted as to whether a data protection impact assessment is required, and if so how to undertake that assessment.

16 Disclosure and sharing of personal information

16.1 We may share personal data that we hold about data subjects without their consent with other organisations. Such organisations include the Department for Education, and Education and Skills Funding Agency "ESFA", Ofsted, health authorities and professionals, the Local Authority, examination bodies, other schools and other organisations where we have a lawful basis for doing so.

16.2 The Rivers C of E Academy Trust will inform data subjects of any sharing of their personal data unless we are not legally required to do so, for example where personal data is shared with the police in the investigation of a criminal offence.

16.3 Where appropriate, and in line with the Data (Use and Access) Act 2025,

the Trust may also share or grant access to personal data through Trusted Research Environments (TREs) or accredited secure data-sharing platforms. Any such arrangements will be subject to governance, audit, and risk assessments, and will be documented within the Trust's Records of Processing Activities (RoPA). Consent may not always be required for these types of lawful access, but data minimisation and proportionality principles will always apply.

16.4 In some circumstances we will not share safeguarding information. Please refer to our Child Protection Policy.

16.5 Further detail is provided in our Schedule of Processing Activities.

17 Data Processors and Data Sub Processors

17.1 We hold contracts with various organisations who provide services to the Trust or School, including:

17.1.1 Providers of school meals, school milk, cashless payment systems, communication systems such as text messaging, pupil photographs and other goods and services where data is required to supply the service;

17.1.2 Providers of online curriculum software that requires individual identification.

17.1.3 Information sent for statutory returns such as SATs results, census returns.

17.1.4 Providers of human resources consultancy, employee contract services, payroll and other business support services;

17.1.5 Providers of secure destruction or storage of data such as Microsoft cloud storage, management information systems, secure shredding;

17.2 In order that these services can be provided effectively we are required to transfer personal data of data subjects to these data processors.

17.3 Personal data will only be transferred to a data processor if they agree to comply with our procedures and policies in relation to data security, or if they put in place adequate measures themselves to the satisfaction of the Trust or School. The Rivers C of E Academy Trust will always undertake due diligence of any data processor before transferring the personal data of data subjects to them.

17.4 Contracts with data processors will comply with Data Protection Legislation and contain explicit obligations on the data processor to ensure compliance with the Data Protection Legislation, and compliance with the rights of Data Subjects.

17.5 Data Processors may use Data Sub Processors. The Data Processor must ensure the Sub-Processor provides the exact level of data security as the

Data Processor does with the Data Controller.

18 Record of Processing Activities (RoPA)

18.1 The Rivers CofE Academy Trust keep a Record of Processing Activities (RoPA). The RoPA includes:

- our organisation's name and contact details, whether it is a controller or a processor (and where applicable, the joint controller, their representative and the DPO);
- the purposes of the processing;
- a description of the categories of individuals and of personal data;
- the categories of recipients of personal data;
- details of transfers to third countries, including a record of the transfer mechanism safeguards in place;
- retention schedules; and
- a description of the technical and organisational security measures in place.

18.2 The RoPA will also record any data sharing carried out through Trusted Research Environments or secure data-sharing platforms, in accordance with the Data (Use and Access) Act 2025. This includes the nature of the data accessed, the parties involved, the lawful basis, and the safeguards applied.

19 Images and Videos

19.1 Parents and others attending Rivers C of E Academy Trust events are allowed to take photographs and videos of those events for domestic purposes under Headteacher's discretion. For example, parents can take video recordings of a school performance involving their child under the Headteacher's discretion. The Rivers C of E Academy Trust does not prohibit this as a matter of policy.

19.2 The Rivers C of E Academy Trust does not however agree to any such photographs or videos being used for any other purpose, but acknowledges that such matters are, for the most part, outside of the ability of the Rivers C of E Academy Trust to prevent.

19.3 The Rivers C of E Academy Trust asks that parents and others do not post any images or videos which include any child other than their own child on any social media or otherwise publish those images or videos.

19.4 As Rivers C of E Academy Trust we want to celebrate the achievements of our pupils and therefore may want to use images and videos of our pupils within promotional materials, or for publication in the media such as local, or even national, newspapers covering school events or achievements. We will seek the consent of pupils, and their parents

where appropriate, before allowing the use of images or videos of pupils for such purposes.

19.5 Whenever a pupil begins their attendance at the Rivers C of E Academy Trust they, or their parent where appropriate, will be asked to complete a consent form in relation to the use of images and videos of that pupil. We will not use images or videos of pupils for any purpose where we do not have consent.

20 CCTV

20.1 The Rivers C of E Academy Trust operates a CCTV system on some school sites. Please refer to the school's own CCTV Procedures.

21 Data Breaches

21.1 A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches resulting from both human error and cyber incidents.

21.2 All suspected or actual data breaches must be reported immediately to the Data Protection Officer (DPO), who will assess the risk to individuals and determine whether the breach must be reported to the Information Commissioner's Office (ICO) within 72 hours.

21.3 The Trust maintains a Data Breach Procedure which outlines the steps to be taken in the event of a breach, including:

- Initial containment and recovery actions
- Risk assessment and classification
- Notification of affected individuals (if required)
- Recording the breach and any remedial actions in the Trust's Data Breach Log

21.4 Staff are required to complete data protection training annually and must report all incidents, even if they are unsure whether they constitute a breach.

21.5 The DPO is responsible for oversight of breach management, audit, and reporting.

22 Monitoring and Review of Compliance

23.1 The Rivers CofE Academy Trust monitors compliance with data protection policies and procedures through a range of mechanisms including:

- Annual reviews of the Trust's Record of Processing Activities (RoPA)
- Audits of data sharing, data breach incidents, and Subject Access Requests
- Review of Data Protection Impact Assessments (DPIAs)
- Ongoing liaison between the Data Protection Officer (DPO), school leads, and service providers
- Use of logs and records (e.g. SAR log, breach log, data processor due diligence log)

23.2 Findings from these activities are reported to the Audit, Risk and Compliance Committee and are used to inform policy updates and staff training priorities.

23 Changes to this policy

We may change this policy at any time. Where appropriate, we will notify data subjects of those changes.

Use link below for additional non-statutory advice from the Department for Education regarding biometric information about pupils for the purposes of using automated biometric recognition systems: D:\Policies\Protection_of_Biometric_Information.pdf

ANNEX

DEFINITIONS

Term	Definition
Data	is information which is stored electronically, on a computer, or in certain paper-based filing systems
Data Subjects	for the purpose of this policy include all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information
Personal Data	means any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
Data Controllers	are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes
Data Users	are those of our workforce (including Local Governors, Trustees and volunteers) whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times
Data Processors	include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions
Data Sub-Processor	is a **third-party data processor** engaged by a Data Processor who has or will have access to or process personal data from a Data Controller. In order to use a sub-processor, the processor needs to have the controller's written permission.
Processing	is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties
Record of Processing Activities (RoPA)	is an active document that requires regular reviews and updates to guarantee adherence to GDPR, especially when processing includes special categories of data. GDPR Article 30 mandates organizations to maintain a RoPA, a document that records their personal data processing activities.

Special Category Personal Data	includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data
Workforce/Staff	Includes, any individual employed by The Rivers C of E Academy Trust such as staff and those who volunteer in any capacity including parent helpers, community volunteers, local Governors, Trustees and Members

Summary of Changes

Date	Section	New Paragraph Number	Summary of Change
June 2025	2 – About this Policy	N/A	Reference to Data (Use and Access) Act 2025
June 2025	6 – Fair and Legal Processing	6.4.5	New legal basis added
June 2025	12 – Rights of the Data Subject	12.1.8	Paragraph explaining the new right for data subjects to be informed when their data is accessed under the 2025 Act, including limits and exemptions.
June 2025	14 – Cyber Security	14.1A	Expanded this section to list specific security controls (e.g. 2FA, cloud backups, phishing protection, endpoint security, penetration testing) and to reference the principle of "privacy by design and by default".
June 2025	16 – Disclosure and Sharing of Personal Information	16.2A	Paragraph introducing the use of Trusted Research Environments (TREs) and secure data platforms for

			lawful data access under the 2025 Act.
June 2025	17 – Data Processors and Data Sub-Processors	17.6	Clarification that sub-processors must be authorised by the Trust in writing, match all data protection obligations, and be included in the RoPA. Ongoing due diligence is required.
June 2025	18 – Record of Processing Activities (RoPA)	18.2	Paragraph requiring the RoPA to include records of data sharing through TREs and similar platforms, with appropriate safeguards.
June 2025	22- Data Breaches	22.1–22.5	New section defining personal data breaches, outlining reporting obligations, ICO notification procedures, internal logging, and the responsibilities of the DPO and staff in managing breaches.
June 2025	23 – Monitoring and Review of Compliance	23.1-23.2	New section outlining how the Trust monitors and reviews compliance with data protection obligations, including audits, RoPA reviews, and committee reporting.