The Rowan Learning Trust

POLICY NAME: **Data Protection Policy**

ADOPTED: Autumn Term 2024

REVIEW PERIOD: Annually

REVIEWER: Director of Risk and Compliance

MAXIMISING POTENTIAL

Policy Document Version Control

Version 1

Responsibility for Policy:	Data Protection Officer
Policy approval/date:	July 23 (trust)
Frequency of Review:	Annual
Next Review date:	July 2024
Related Policies:	Data Breach policy Information Security Policy SARS policy FOI policy Records management policy Retention and destruction policy CCTV policy (all the above policies can be found at Rowan Learning Trust - GDPR & Data Protection - All Documents (sharepoint.com)
Minor Revisions:	**A revision was made on 19th July 2023. On page 15, this policy referred to itself for data breaches. Data breaches have their own policy and this has now been corrected at the bottom of page 15.** **The ICO also recommended a link being applied to the policy and that has now been rectified by adding the link the 'related policies' section of this version control document.**

Version 2

Responsibility for Policy:	Data Protection Officer
Policy approval/date:	July 23 (trust)
Frequency of Review:	Annual
Next Review date:	July 2024
Related Policies:	Data Breach policy Information Security Policy SARS policy FOI policy Records management policy Retention and destruction policy CCTV policy (all the above policies can be found at Rowan Learning Trust - GDPR & Data Protection - All Documents (sharepoint.com)
Minor Revisions:	**On 8th February 2024, a link to the Records Management policy was added on to the start of section 13.**

Version 3

Responsibility for Policy:	Data Protection Officer
Policy approval/date:	July 23 (trust)
Frequency of Review:	Annual
Next Review date:	July 2024
Related Policies:	Data Breach policy Information Security Policy SARS policy FOI policy Records management policy Retention and destruction policy CCTV policy (all the above policies can be found at Rowan Learning Trust - GDPR & Data Protection - All Documents (sharepoint.com)
Minor Revisions:	**On 9th February a sentence was added to point 12.8 directing anyone who to contact should they feel that they need their data rectifying.**

Version 4

Responsibility for Policy:	Data Protection Officer
Policy approval/date:	July 23 (trust)
Frequency of Review:	Annual
Next Review date:	July 2024
Related Policies:	Data Breach policy Information Security Policy SARS policy FOI policy Records management policy Retention and destruction policy CCTV policy (all the above policies can be found at Rowan Learning Trust - GDPR & Data Protection - All Documents (sharepoint.com)
Minor Revisions:	**On 14th February a link has been added for the data sharing policy and mentioned in point 15.1 (click the link below)** Disclosure and sharing of personal information

Version 5

Responsibility for Policy:	Data Protection Officer
Policy approval/date:	July 23 (trust)
Frequency of Review:	Annual
Next Review date:	July 2024
Related Policies:	Data Breach policy Information Security Policy SARS policy FOI policy Records management policy Retention and destruction policy CCTV policy (all the above policies can be found at Rowan Learning Trust - GDPR & Data Protection - All Documents (sharepoint.com)
Minor Revisions:	**17th Sept 2024 extra regarding rights to rectification was added to**

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 a Trust, we and our schools 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 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.

1.4 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.

1.5 All members of our workforce receive training and regular updates on best practice for handling personal data.

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 (together '**Data Protection Legislation**').

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. Roles and Responsibilities

3.1 **Trust Board is responsible for:** The Trust Board of Trustees (through its Local Governing Committees) has overall responsibility for ensuring that our organisation complies with all relevant data protection obligations.

3.2 **Data Protection Officer is responsible for:** The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection l aw, and developing related policies and guidelines where applicable.

3.2.1 They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on Trust data protection issues.

3.2.2 The DPO is also the first point of contact for individuals whose data the Trust processes, and for the ICO. Full details of the DPO's responsibilities are set out i n their job description.

3.2.3 Our DPO is Chris Bolton and is contactable at DPO@rlt.education

3.3 **Chief Executive and Headteachers are responsible for:** The CEO,Directors of Phase and Headteachers act as the representative of the data controller on a day-to-day basis.

3.4. **All Staff are responsible for:** Collecting, storing and processing any personal data in accordance with this policy

3.4.1 Informing the Trust of any changes to their personal data, such as a change of address
3.4.2 Contacting the DPO in the following circumstances:
3.4.3 With any questions about the operation of this policy, data protection l aw, retaining personal data or keeping personal data secure
3.4.4 If they have any concerns that this policy is not being followed
3.4.5 If they are unsure whether they have a lawful basis to use personal data in a particular way
3.4.6 If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
3.4.7 If there has been a data breach
3.4.8 Whenever they are engaging i n a new activity that may affect the privacy rights of Individuals
3.4.9 If they need help with any contracts or sharing personal data with third parties

4. **Definition of data protection terms**

Term	Definition
Data	is information which is stored electronically, on a computer, or in certain paperbased 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 Governors 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
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
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	Includes, any individual employed by [School/Trust/Academy] such as staff and those who volunteer in any capacity including Governors [and/or Trustees / Members/ parent helpers]

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 the Trust and our schools.

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.**

6.5 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 Trust or a Trust school 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 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 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 Trust/School, 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

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.

10.3 **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.

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 schools 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 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 Trust or one of our schools that **personal data** held about them by the Trust or School is inaccurate or incomplete then we will consider that request and provide a response within one month. To do this, a data subject must contact the Trust Data Protection Officer at dpo@rlt.education

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.

Article 16 of the General Data Protection Regulations (GDPR) states "The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement."

One of the principles of GDPR is for our Trust to ensure that the data we hold be 'accurate and, where necessary, kept up to date', and we must take every reasonable step to ensure that we follow this principle. To this end, we provide users with the capability to directly update some of their information directly and will always ask students to update their personal information at the start of each year.

When it applies

If personal data is inaccurate, contains expressions of opinion based on inaccurate information, or if it is incomplete, then individuals have the right to have that data rectified, or to have a marker placed on it to show any corrections.

How will our Trust react?

If the University has made the information available to third-party, we must make them aware that you have exercised this right and ensure that they also take appropriate actions with the relevant information.

For paper based systems

- Information in the file should be corrected or replaced.
- A note should be placed on the individual file to show that the record has been 'rectified' or disputed and not rectified.

For automated systems

- The rectification should in principle be ensured by technical means specific to the systems.
- Where the system is a data source, rectification should cascade through all relevant systems in the data flow.

How long does our Trust have to comply?

Where it is required for us to do so, we must make the rectifications without any undue delay and certainly no longer than a month from the date of your request.

Can timescale be extended?

Yes – if the request is complicated, we can extend for a further two months, but we will let you know if this is the case within the original timescale.

Is there a fee?

No.

How does some request a rectification?

You may submit a request to have data rectified to any member of staff, in a number of different ways, including via telephone or in person, but please be clear when you tell us:

- What data you are asking to have rectified.
- What you believe is inaccurate.
- What the correct version of the data should be.

If you have any issues or queries, please contact the University Data Protection Officer:

Phone number: 01942 939022
Email: dpo@rlt.education

Write to: Senior Information Risk Officer, 18 Beecham Court, Wigan. WN3 6PR

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 Trust/School can continue to hold the **personal data** but not do anything else with it.

12.12 The Trust/School 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 Trust/School 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 Trust/School not to delete the **personal data**; and

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

12.13 If the Trust/School 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 Trust/School 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 Trust/School 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 Trust/School 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 Trust/School 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

please refer to the RM policy for further security measures.

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 the main office, or a member of the senior leadership team.

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.)

13.3.3 **Methods of disposal.** Paper documents should be shredded or placed in a secure confidential waste bin for collection. 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, and in accordance with the Trust policy on disposal of IT assets.

13.3.4 **Equipment.** Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from or lock their PC when it is left unattended.

13.3.5 **Working away from the school premises – paper documents.** Further details can be found in the RLT Remote Working policy

13.3.6 **Working away from the school premises – electronic working.** All devices containing personal information must be encrypted before leaving the school / Trust premises. Further details can be found in the RLT Remote Working policy

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

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

14. Data Protection Impact Assessments

14.1 The 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.

14.2 In certain circumstances the law requires us to carry out detailed assessments of proposed **processing**. This includes where we intend to use new technologies which might pose a high risk to the rights of **data subjects** because of the types of data we will be **processing** or the way that we intend to do so.

14.3 The Trust/School will complete an assessment of any such proposed **processing** and has a template document which ensures that all relevant matters are considered.

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

15. Disclosure and sharing of personal information

15.1 We may share **personal data** that we hold about **data subjects**, and without their consent, with other organisations. Such organisations include the Department for Education, and / or 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.

15.2 The Trust/School 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.

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

15.4 Further detail is provided in our data sharing policy (link provided above)

16. Data Processors

16.1 We contract with various organisations who provide services to the Trust and our schools, including:

16.1.1 Payroll providers, catering providers, providers of online systems for assessment, tracking, monitoring and safeguarding.

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

16.3 **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/School. The Trust/School will always undertake due diligence of any **data processor** before transferring the **personal data** of **data subjects** to them.

16.4 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. Images and Videos

17.1 Parents and others attending Trust/School events are allowed to take photographs and videos of those events for domestic purposes. For example, parents can take video recordings of a school performance involving their child. The Trust/School does not prohibit this as a matter of policy.

17.2 The Trust/School 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 Trust/School to prevent.

17.3 The Trust/School 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.

17.4 As a Trust/School 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.

17.5 Whenever a pupil begins their attendance at the Trust/School 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.

18. **CCTV**

18.1 The Trust/School operates a CCTV system. Please refer to the Trust CCTV Policy

19. Remote Working

19.1 **Remote Access**

19.1.2 Remote Access is the preferred method for staff wishing to work remotely. Data is securely stored on a server within Trust premises, so it cannot be misplaced or lost. It is also regularly backed up.

19.1.3 Remote access can be accessed on both corporate and personal devices. Please refer to the remote access policy for further details.

19.1.4 Access to printers, USB devices and the clipboard is restricted, so the possibility of data loss is minimised.

19.2 **Taking Documents Home**

19.2.2 Documents with little personal data, such as student work books or coursework, are suitably low-risk and can be taken home by staff without additional precautions. This is reasonable and practical, and allows teachers to mark work more easily.

19.3 **Documents with substantial amounts of personal data**

19.3.1 Documents with more substantial amounts of personal data need additional scrutiny in how they are handled. These may include

19.3.2 Pupil records

19.3.3 Annual or termly pupil reports

19.3.4 Higher or further education references

19.3.5 Confidential financial / HR information

19.4 Each department should establish a sign-out and sign-in system, so it is clear where the documents are and who has them.

19.5 Documents should be kept in a closed folder, such as one with a zip lock. Staff should include their name and contact details in case the folder is lost

19.6 If taken home, the documents should be kept in a secure area of the house. They should be kept in a particular place, such as a certain drawer or tray, to prevent them being lost.

19.7 Staff should not leave documents in a vehicle

19.8 When returning the documents, staff should immediately take the documents to their original storage place, rather than leaving them on a desk to return later.

Any suspected data breaches should be reported immediately to the Trust data protection officer. See the Trust Data Breach policy for more information.