THE PATHWAY ACADEMY TRUST
Registered address: c/o Culverstone Green Primary School,
Wrotham Road, Meopham, Kent DA13 0RF
Registered Company N° 9782388

DATA PROTECTION POLICY

Author	**Trust Business Manager**
Approved by	**Trust Board**
Version	**1.0**

Contents

Statement of Intent 2
Legal Framework 2
Definitions and Applicable Data 2
Principles 3
Accountability 3
Data Protection Officer (DPO) 4
Lawful Processing 4
Consent 5
The Right to be Informed 6
The Right of Access 6
The Right to Rectification 8
The Right to Erasure 8
The Right to Restrict Processing 9
The Right to Data Portability 9
The Right to Object 10
Privacy by Design and Privacy Impact Assessments 11
Data Breaches 12
Data Security 13
Publication of Information 16
CCTV and Photography 16
Data Retention 17
Disclosure and Barring Service (DBS) Data 17
Right to Work Documents 17

Statement of Intent

The Pathway Academy Trust and its schools are required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the General Data Protection Regulation (GDPR). This is the law that protects personal privacy and upholds individuals' rights. It applies to anyone who handles or has access to people's personal data.

The Trust or its schools may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the Department for Education, the local authority, other schools and educational bodies, or social services.

This policy is in place to ensure that personal information is dealt with properly and securely, and in accordance with the GDPR and UK data protection legislation. It will apply to information regardless of the way it is used, recorded or stored, and whether it is held in paper files or electronically. This policy is also to ensure that all staff and governance bodies are aware of their responsibilities, and it outlines how the Trust and schools comply with the core principles of the GDPR.

Legal Framework

This policy has due regard to legislation, including, but not limited to the following:

- The General Data Protection Regulation (GDPR)
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998

This policy will also have regard to guidance from the Information Commissioner's Office.

This policy will be implemented in conjunction with other Trust policies, including, but not limited to:

- TPAT Records Management Policy
- IT Acceptable Use Policy

Definitions and Applicable Data

For the purpose of this policy, **personal data** refers to any information that relates to an identified or identifiable natural (living) individual, who can be identified, directly or indirectly, by reference to an identifier (such as a name), location data, an online identifier (such as an IP address), or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. The GDPR applies to automated personal data and to manual filing systems, as well as to chronologically ordered data and pseudonymised data (such as Unique Pupil Numbers or National Insurance numbers). It also includes any expression of opinion about an individual, intentions towards an individual, and personal data held visually in photographs or video clips (including CCTV) or as sound recordings.

Sensitive personal data is referred to in the GDPR as '**special categories of personal data**'. These specifically include the processing of genetic data, biometric data and data concerning health matters.

An individual about whom such information is stored is known as the **data subject**. Data subjects include employees, pupils, parents, visitors, contractors and local governors. The organisation storing and controlling such information (The Pathway Academy Trust) is referred to as the **data controller**. The Trust decides how and why the information is used, and has a responsibility to establish workplace practices and policies that are in line with the GDPR.

Principles

In accordance with the requirements outlined in the 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 is 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 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 GDPR requires that 'the controller shall be responsible for, and able to demonstrate, compliance with [these] principles'.

Accountability

The Pathway Academy Trust, as a corporate body, is named as the data controller under the GDPR. The Trust has a legal duty to comply with the regulations, including:

- The Trust will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.
- The Trust will inform data subjects why they need their personal information, how they will use it, and with whom it may be shared. To this end, the Trust will provide comprehensive, clear and transparent privacy policies for both staff and parents (on behalf of pupils).

- Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or that in relation to criminal convictions and offences.
- Internal records of processing activities will be in the form of a data audit and include the following:
    - Description of the personal data
    - Purpose(s) of the processing
    - Any recipients of the personal data
    - Description of technical and organisational security measures
    - Details of any transfers to third countries, including documentation of the transfer mechanism safeguards in place
- The Trust will implement measures that meet the principles of data protection by design and data protection by default, such as:
    - Data minimisation
    - Pseudonymisation
    - Transparency
    - Allowing individuals to monitor processing
    - Continuously creating and improving security features
- Data protection impact assessments will be used, where appropriate.
- The Trust will ensure that every member of staff that holds personal information understands that they must comply with the GDPR when managing that information.

Data Protection Officer (DPO)

A DPO will be appointed in order to:

- Inform and advise the Trust, schools and its employees about their obligations to comply with the GDPR and other data protection laws
- Monitor the Trust's and its schools' compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members
- The role of DPO will be outsourced to the General Data Protection Regulation in Schools (GDPRiS) DPO service, provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests
- The DPO will have professional experience and knowledge of data protection law, particularly that in relation to schools
- The DPO will report to the highest level of management at the Trust, which is the Board of Directors, via the Trust Business Manager
- 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 GDPR obligations, including support from Data Compliance Leads in each school

Lawful Processing

The legal basis for processing data will be identified and documented prior to data being processed.

Under the GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained, or
- Processing is necessary for:
    - Compliance with a legal obligation
    - The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
    - For the performance of a contract with the data subject or to take steps to enter into a contract
    - Protecting the vital interests of a data subject or another person
    - For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject

Special categories of personal data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State 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 Union or Member State 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 services on the basis of Union or Member State law or a contract with a health professional
    - 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)

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. Consent can be withdrawn by the individual at any time.

The consent of parents will be sought prior to the processing of a child's data, where the age threshold is considered to be 13 years of age.

The Trust will ensure that consent mechanisms meet the standards of the 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.

The Right to be Informed

The privacy notices 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.

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 contact details of the Trust and its DPO
- The purpose of, and the legal basis for, processing the data
- The legitimate interests of the controller
- Any recipient or categories of recipients of the personal data
- Details of any transfers to third countries and the safeguards in place, if applicable
- Details of where to find the retention periods
- The existence of the data subject's rights, including the right to:
    - Withdraw consent at any time
    - Lodge a complaint with a supervisory authority

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. This information will be supplied at the time the data is obtained.

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 if possible. 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 is disclosed
- If the data are used to communicate with the individual, at the latest, when the first communication takes place

The Right of Access

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

Requests must be made in writing and addressed to the Head Teacher of the school. If the initial request does not clearly identify the information required, further enquiries will be made.

The school will verify the identity of the person making the request before the disclosure of any personal information, and checks should also be carried out regarding proof of relationship to the child if applicable. Evidence of identity can be established by requesting production of one or more of the following (this list is not exhaustive):

- Passport
- Driving licence
- Utility bills with the current address
- Birth or marriage certificate
- P45 or P60
- Credit card or mortgage statement

Any individual has the right of access to information held about them. However with children, this is dependent upon their capacity to understand. As a general rule, a child of 13 or older is expected to be mature enough to understand the request they are making. If the child cannot understand the nature of the request, someone with parental responsibility can ask for the information on the child's behalf. If appropriate, the Head Teacher should discuss the request with the child and take their views into account when making a decision.

All subject access requests will be dealt with in line with the Subject Access Code of Practice and other guidance from the Information Commissioner's Office.

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

Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

Information can be viewed at the school with a member of staff on hand to help and explain matters if requested, or provided at a face-to-face handover.

Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee may be charged. All fees will be based on the administrative cost of providing the information.

All 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 will 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.

Where a request is manifestly unfounded or excessive, the Trust 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 supervisory authority and to a judicial remedy, within one month of the refusal.

In the event that a large quantity of information is being processed about an individual, the Trust will ask the individual to specify what information the request is in relation to.

There are some exemptions to the right to subject access that apply in certain circumstances or to certain types of personal information. **Therefore, all information must be reviewed prior to disclosure**. If there are concerns over the disclosure of information, then additional advice will be sought from the Trust Business Manager, who may consult with the Trust's Data Protection Officer.

Where redaction (where information has been edited or removed) has taken place, then a full copy of the information provided will be retained in order to establish, if a complaint is made, what was redacted and why.

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 Trust will inform them of the rectification where possible.

Where appropriate, the Trust 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 a further two months where the request for rectification is complex.

Where no action is being taken in response to a request for rectification, the Trust will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

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 or 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 any Information Society services (that is, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services)

The Trust 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

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 Trust will inform other organisations who process the personal data to erase links to, and copies of, the personal data in question.

The Right to Restrict Processing

Individuals have the right to block or suppress the Trust's processing of personal data.

In the event that processing is restricted, the Trust 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 Trust 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 Trust has verified the accuracy of the data
- Where an individual has objected to the processing and the Trust is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restriction instead
- Where the Trust 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 Trust 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 Trust will inform individuals when a restriction on processing has been lifted.

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 Trust will provide the information free of charge.

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

The Pathway Academy Trust 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 Trust will consider whether providing the information would prejudice the rights of any other individual.

The Trust 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 a further 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 Trust 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.

The Right to Object

The Trust will inform individuals of their right to object at the first point of communication, and 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
- Direct marketing
- 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 Trust will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the Trust can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual

It is the Trust's policy not to engage in direct marketing activities, such as putting leaflets in school bags. Instead, offers and information will be made available to pupils and their families in the schools' reception areas.

If personal data is ever processed for direct marketing purposes:

- The Trust will stop processing personal data for direct marketing purposes as soon as an objection is received
- The Trust 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 Trust is not required to comply with an objection to the processing of the data

Privacy by Design and Privacy Impact Assessments

The Trust will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the Trust 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 Trust's data protection obligations and meeting individuals' expectations of privacy.

DPIAs will allow the Trust to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to The Pathway Academy Trust'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 Trust 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

Where a DPIA indicates high risk data processing, the Trust will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

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.

The Trust Business Manager, with support from the school Data Compliance Leads, 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 relevant supervisory authority (the Information Commissioner's Office) will be informed by the Trust's Data Protection Officer. Any notifiable breach will be reported to the Information Commissioner's Office within 72 hours of the Trust becoming aware of it.

The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis by the Trust Business Manager and Trust's Data Protection Officer.

In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the Trust will notify those concerned directly.

A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

In the event that a breach is sufficiently serious, relevant third parties such as other regulatory bodies, the police, the media, or the public will be notified without undue delay.

Effective and robust breach detection, investigation and internal reporting procedures are in place at the Trust, which facilitate decision-making in relation to whether the relevant supervisory authority 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: an assessment of any risks associated with the breach, and in particular the potential adverse consequences for individuals, how serious or substantial these are, and how likely they are to happen
- A description of the proposed measures to be taken to deal with the personal data breach, including a recovery plan if applicable
- Details of the investigation into the causes of the breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

Following a data breach, the causes of the breach will be fully investigated, and the effectiveness of the Trust's response to the breach will be evaluated.

Data Security

All staff members will take all reasonable steps to ensure personal data is kept secure, including the following measures:

Paper Records

- Paper records containing personal information will be kept in a locked filing cabinet, drawer or safe, with restricted access. This includes payslips waiting to be collected.
- Confidential paper records will not be left unattended or in clear view anywhere with general access.
- Documents containing personal or confidential data that have reached the end of their life are disposed of by shredding, which is done promptly and on-site where possible. If an external company is used for shredding, the bulk bags must be locked away when unattended.
- Desks must be clear at the end of the day, or if left unattended.

Remote Access

- Where possible, electronic data is stored where it can be accessed remotely to give the Trust greater control over who accesses it and how.
- Staff will not remain logged in between sessions when using remote access.
- Passwords for remote access are not to be auto-saved on any device.

Electronic Records

- Digital data is encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up.
- 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.
- Memory sticks are only to be used if there is no other means of transferring electronic records (for example, by accessing them from a shared remote area). If memory sticks are used, they must be encrypted, remain on the school site and the files must be deleted immediately after use.

Electronic Devices and Passwords

- All electronic devices, including laptops, tablets and mobile phones, must be password-protected using a strong password to protect the information on the device in case of loss or theft. Strong passwords are at least seven characters long, with a combination of upper- and lower-case letters, numbers and special keyboard characters (such as an asterisk or currency symbol). If an incorrect password is entered too many times, access to the device is locked.
- All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.
- Log on passwords and user IDs must not be shared; however, passwords for shared working documents are acceptable.
- Passwords must not be auto-saved on devices, websites or applications.
- The screens on all devices must be locked when staff are away from the device so that the device is inaccessible to others.
- Devices are set to automatically lock if left inactive for a period of time.

- Documents including personal data should only be sent to printers on release by a code unique to that member of staff. This means that no personal data should be free printed or left on the printers or photocopiers for others to view.
- Device screens must not be able to be viewed by any unauthorised personnel.
- Staff, local governors, directors and members are advised not to use their personal laptops or computers for Trust purposes. Documents should not be downloaded to devices where possible, but if downloaded should be deleted immediately after the meeting.
- Staff must not share any devices that store personal data among their family or friends. If a personal device is used for work purposes and is lost or stolen, the Trust Business Manager must be informed immediately.
- Where possible, the Trust enables the remote blocking or deletion of data stored on a device in case of loss or theft.
- Antivirus software is installed on all Trust and school devices and is kept up-to-date. Prompts for regular scans or updates must not be ignored by members of staff.
- The IT managers ensure that any 'patches' or security updates are downloaded and applied promptly to Trust and school devices to cover any vulnerabilities.
- If personal devices are used for work purposes, anti-virus software must be installed and both the operating system and anti-virus software must be kept up-to-date. This is the responsibility of the owner of the device.

Emails and Fax

- Personal data should not be sent within the body of an email if possible. Ideally, it should be stored securely in an area that can be remotely accessed by all relevant parties. However, if the information is factual and unlikely to cause the data subject any harm in the event of a data breach, it can be sent in the body of an email.
- If it is unavoidable to attach a document that contains personal data to an email, password protection must be enabled on the document and the email must be flagged as confidential (for example, by stating this in the subject line of the email). Personal or confidential information must not be included in the subject field.
- Passwords must be sent separately to the email containing the attachment. Ideally the password should be sent by a separate means, such as by phone call, to avoid emailing the password to the same person in error. If the password is sent by email, the recipient must confirm that they have received the information before the sender sends the password in reply to that email.
- All emails to outside organisations are encrypted as standard.
- Circular emails to parents or any multiple recipients outside of the school or Trust are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
- An audit trail of all email communications is saved. For EIS email accounts this is while the account remains active; for Trust email accounts the record is saved indefinitely.
- If the S2S system is used to share information between schools and local authorities, the common transfer file (CTF) naming protocols must be followed, the data must be saved in an encrypted folder or file, and the file must be sent as a compressed folder.
- When sending personal information by fax, staff will always check that the recipient is correct before sending. Personal information is not sent by fax unless the information has been de-personalised or the fax machine is in a secure area, which is locked when unattended. If it is unavoidable to send personal information by fax, the recipient will

be asked to confirm receipt of the fax and a cover sheet will be used to mark it 'Private and Confidential'.

Off-Site Working

- Personal information is only to be taken off-site in accordance with the guidelines listed below. It must be returned to site as soon as possible.
- Where personal information (including named school books for marking) 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 if possible, keeping documents out of sight, and using travel locks to secure bags.
- Where possible, complete files are not transported – only the relevant documents are taken off-site.
- Vehicles used to transport personal data or mobile devices must be kept locked and secure when unoccupied (even for a short time). Personal information and mobile devices transported in vehicles must be kept hidden in a locked boot wherever possible, or otherwise kept out of sight to avoid opportunist crimes.
- Personal information and mobile devices must not be left in vehicles overnight.
- The person taking the information from the school or Trust premises accepts full responsibility for the security of the data.

Sharing Data

- Before sharing data, all staff members will ensure:
    - They are allowed to share it
    - That adequate security is in place to protect it
    - Who will receive the data has been outlined in a privacy notice
- In particular, personal information must not be given out over the telephone unless this is part of a data sharing agreement with a data processor. Instead, the caller must be invited to put their request in writing. If the request is urgent, the caller's name and switchboard telephone number must be taken and their name, job title and department verified with the switchboard before responding. Mobile phone numbers should only be used if there is no alternative, and these should be verified with the switchboard of the central organisation in the same way if possible.
- Once their details have been confirmed, information is only provided to the person who requested it and a record of any personal information disclosed during the call is added to the pupil or personnel file.
- Personal business is never discussed in public areas or where conversations could be overheard by people with no right to know the details of the information.
- If personal information is sent by post, the responsible member of staff must:
    - Confirm the name, department and address of the recipient
    - Seal the information in a robust envelope
    - Mark the envelope 'Private and Confidential – To be opened by Addressee Only' and place this inside a larger envelope with only the correct name and address on it - this adds an additional level of security as the package is not easily identifiable as 'valuable' and administrative staff should only open the outer envelope
- If special category personal information is sent by post, the responsible member of staff must also:
    - Send the information by recorded, registered or 'signed for' delivery or by a reliable courier where appropriate

- Ask the recipient to confirm receipt
- Record the disclosure on the pupil or personnel file

Visitors

- Under no circumstances are visitors allowed access to confidential or personal information.
- This means that members of staff must be mindful of personal information that is on display in their offices or classrooms (such as pupil names, particularly if linked to special educational needs or health care plans). If meetings with visitors take place in these offices, steps must be taken to cover this information.
- Visitors to areas containing personal information are supervised at all times.

The physical security of the Trust's buildings and storage systems, and access to them, is reviewed on a regular basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

The Pathway Academy Trust takes its duties under the 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.

Publication of Information

The Pathway Academy Trust publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

- Policies and procedures
- Annual reports
- Financial information

Classes of information specified in the publication scheme are made available quickly and easily on request.

The Pathway Academy Trust will not publish any personal information, including photos, on its website without the permission of the affected individual.

When uploading information to the school or Trust websites, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site. For example, text must not be hidden by colouring or highlighting it, and Excel spreadsheets must be checked for hidden columns and rows (as these can still be found in search results or when copying and pasting data). Further guidance on hidden data can be found on the Information Commissioner's Office website.

CCTV and Photography

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

The Trust notifies all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards.

Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

The Head Teachers are responsible for ensuring the records are secure and allowing access.

If the Trust wishes to use images or video footage of pupils in a publication, such as the school website, prospectus, or recordings of school plays, written permission will be sought for the particular usage from the parent of the pupil.

The Trust will always indicate its intentions for taking photographs or video footage of pupils and will retrieve permission before publishing them.

Images captured by individuals for recreational or personal purposes, and videos made by parents for family use, are exempt from the GDPR.

Data Retention

Data will not be kept for longer than is necessary in line with guidelines included in the Trust's Record Management Policy.

Unrequired data will be deleted as soon as practicable.

Some educational records relating to former pupils or employees of the Trust 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, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

Disclosure and Barring Service (DBS) Data

All data provided by the DBS will be handled in line with data protection legislation, which 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.

Right to Work Documents

Copies of documents regarding an individual's right to work in the UK will be copied in line with government guidelines, and will be kept during the applicant's employment and for two years after their employment ceases.