Data Protection Policy

2026 - 2027

‘Because Children Deserve Better’

Reviewed By:	Sarah Howarth, Associate Director of Compliance
Approved By:	Kathryn Parkinson, CEO
Responsible Person:	Sarah Howarth, Associate Director of Compliance
Policy number:	7:2 V4
Date:	May 2026
Next Review Date:	May 2027

Contents

1. Aims
2. Legislation and guidance
3. Definitions
4. The data controller
5. Roles and responsibilities
6. Data protection principles
7. Collecting personal data
8. Sharing personal data
9. Subject access requests and other rights of individuals
10. Parental requests to see the educational record
11. CCTV
12. Photographs and videos
13. Artificial intelligence (AI)
14. Data protection by design and default
15. Data security and storage of records
16. Disposal of records
17. Personal data breaches
18. Complaints
19. Training
20. Monitoring arrangements
21. Links with other policies
22. Appendix 1: Personal data breach procedure

1. Aims

Pivot aims to ensure that all personal data collected about staff, learners, parents and carers, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

Relevant legislation includes but is not limited to:

- UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018
- Data (Use and Access) Act 2025 (DUAA)
- ICO guidance on UK GDPR, surveillance and subject access requests (SAR)
- Department for Education guidance on AI in education

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation

Term	Definition
Processing	Anything that is done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual and also includes transmitting or transferring personal data to third parties.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing personal data. The data controller is responsible for establishing practices and policies in line with UK GPDR.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller. A data processor acts only on the instructions of the controller and does not determine the purposes or means of the processing.
Personal data breach	A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. Data controller

Pivot processes personal data relating to parents and carers, learners, staff, visitors and others and therefore is a data controller.

Pivot has paid its data protection fee to the ICO, as legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by Pivot, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Board of Directors

The board has overall responsibility for ensuring that Pivot complies with all relevant data protection obligations.

Data protection officer (DPO)

The DPO is responsible for overseeing the implementation of this policy, monitoring Pivot's compliance with data protection law, and developing related policies and guidelines where applicable.

The DPO will provide a termly report of their activities to the directors and, where relevant, their advice and recommendations on Pivot data protection issues.

The DPO is also the first point of contact for individuals whose data Pivot processes, and for the ICO.

Our DPO is Sarah Howarth and is contactable via sarah.howarth@pivot-group.co.uk.

Please contact the DPO with any questions about the operation of this data protection policy or the UK GDPR, or if you have any concerns that this data protection policy is not being or has not been followed.

Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis and is responsible for ensuring that their team read and understand this policy before carrying out tasks that involve handling personal data and that they follow this policy, including reporting any suspected breaches of it.

All staff

Staff are responsible for:

- Reading and understanding this policy before carrying out tasks that involve handling personal data and for following this policy, including reporting any suspected breaches of it to the DPO
- Collecting, storing and processing any personal data in accordance with this policy
- Informing Pivot of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether they have a lawful basis to use personal data in a particular way
    - 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 UK
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

We adhere to the principles relating to processing of personal data set out in the UK GDPR, which requires personal data to be:

- Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency)
- Collected for specified, explicit and legitimate purposes (purpose limitation)
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed (data minimisation)
- Accurate and, where necessary, kept up to date (accuracy)
- Kept for no longer than is necessary for the purposes for which it is processed (storage

limitation)

- Processed in a way that ensures it is appropriately secure (security, integrity and confidentiality)
- Not transferred to another country without appropriate safeguards in place (transfer limitation)
- Handled in a way that respects the rights of data subjects and allows them to exercise those rights (data subject rights and requests)

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (accountability).

This policy sets out how Pivot aims to comply with these principles.

7. Collecting personal data

Lawfulness, fairness and transparency

We will only process personal data where we have 1 of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that Pivot can fulfil a contract with the individual, or the individual has asked Pivot to take specific steps before entering into a contract
- The data needs to be processed so that Pivot can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual or another person i.e. to protect someone's life
- The data needs to be processed so that Pivot can perform a task in the public interest or exercise its official authority
- The data needs to be processed for the legitimate interests of the organisation or a third party, provided the individual's rights and freedoms are not overridden
- The individual (or their parent/carer when appropriate in the case of a learner) has freely given clear consent

For special categories of personal data, we will also meet 1 of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a learner) has given explicit consent
- The data needs to be processed to perform or exercise obligations or rights in relation to employment, social security or social protection law
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made manifestly public by the individual
- The data needs to be processed for the establishment, exercise or defence of legal claims
- The data needs to be processed for reasons of substantial public interest as defined in legislation

- The data needs to be processed for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for archiving purposes, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a learner) has given consent
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made manifestly public by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights
- The data needs to be processed for reasons of substantial public interest as defined in legislation

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect or use personal data in ways which have unjustified adverse effects on them.

Limitation, minimisation and accuracy

- We will only collect personal data for specified explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.
- If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.
- Staff must only process personal data where it is necessary in order to do their jobs.
- We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.
- In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with Pivot's record retention schedule.

8. Sharing personal data

Generally, we are not allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put in place.

There will be certain circumstances where we may be required to share personal data. These include, but are not limited to, situations where:

- There is an issue with a learner or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and learners – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors that can provide sufficient guarantees that they comply with UK data protection law
    - Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service
- We will also share personal data with law enforcement and government bodies where we are legally required to do so
- We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our learners or staff

Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

9. Subject access requests and other rights of individuals

Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that Pivot holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual

- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request in any form, which may include a text message, through social media, over the phone or face to face, they must immediately forward it to the DPO.

Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of learners at Pivot may be granted without the express permission of the learner. This is not a rule, and a learner's ability to understand their rights will always be judged on a case-by-case basis.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of learners at Pivot may not be granted without the express permission of the learner. This is not a rule and a learner's ability to understand their rights will always be judged on a case-by-case basis.

The consent of our learners (candidates) is sought to share results or other exam related information with third parties.

Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant). Pivot holiday periods, bank holidays and weekends are all included within the 1 month timeframe.
- Will provide the information free of charge
- Pause deadlines ('stop the clock') whilst clarification on the request is being sought
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the learner or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests

- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent, and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it or charge a reasonable fee to cover administrative costs. We will consider whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why and tell them they have the right to complain to the ICO, or they can seek to enforce their subject access right through the courts.

Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Receive certain information about the data controller's processing activities
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing that has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- Be notified of a data breach (in certain circumstances)
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Parental requests to see the educational record

In law there is no automatic parental right of access to their child's educational record as Pivot is an Independent School. However, we want to work in partnership with parents. Parents should put in writing their request and send it to their child's headteacher. An initial response to the request will be made within 5 working days. At this time, we will also give a clear indication of the timeframe in which a full response can be made.

11. CCTV (including site and minibus CCTV systems)

Pivot operates CCTV and video surveillance systems at our sites and within our minibus fleet. CCTV is used only where it is necessary, proportionate and justified, and Pivot has completed, where applicable, a Data Protection Impact Assessment (DPIA) or Legitimate Impact Assessment (LIA) for surveillance systems.

Pivot does not routinely use audio recording and it is enabled only where strictly necessary and documented in a DPIA.

CCTV systems may include access to live (real-time) images by authorised staff where necessary to support safeguarding, health and safety or the management of incidents. Live viewing is not used for continuous or routine monitoring and is accessed only on a case-by-case basis where there is a clear operational need.

CCTV footage is stored securely and access to both live and recorded CCTV is restricted to trained and authorised staff with a defined operational need. All access is logged and subject to periodic review. Technical and organisational measures protect the system from unauthorised access.

Footage may be shared with law enforcement agencies, insurers, legal representatives, local authorities or regulators where lawful and necessary. Pivot ensures any disclosure is documented and proportionate.

CCTV (including live access) will not be used for routine monitoring of staff or learners, or for performance management purposes, unless required as part of a specific and justified investigation.

12. Photographs and videos

As part of Pivot activities, we may take photographs and record images of individuals within our settings.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and the learner.

Any photographs and videos taken by parents/carers at Pivot events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other learners are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

Where Pivot takes photographs and videos, uses may include:

- Within school on notice boards and in Pivot brochures, newsletters etc.
- Outside of Pivot by external agencies such as a photographer, newspapers, campaigns
- Online on our Pivot website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further, including removing from our website if necessary.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

13. Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, learners and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini. Pivot recognises that AI has many uses to help learners learn but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, Pivot will treat this as a data breach and will follow the personal data breach procedure outlined in appendix 1.

Further guidance on the use of AI can be found in Pivot's Use of Artificial Intelligence (AI) Policy, which can be accessed on the internal SharePoint system. The policy can also be made available to parents upon request.

14. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing data protection impact assessments where Pivot's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test Pivot privacy measures and make sure we are compliant
- Appropriate safeguards in place if we transfer any personal data outside of the UK, where different data protection laws may apply
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of the Pivot setting and DPO, and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-

party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure.

15. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office using the appropriate template supplied by the DPO
- Passwords made up of 4 random, unrelated words, or that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and learners are reminded that they should not reuse passwords from other sites. Enable single sign-on (SSO) arrangements where possible.
- Encryption software is used to protect all portable devices and removable media, such as laptops, mobile phones and USB devices
- Staff and learners do not store personal information on their work devices
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

16. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records and overwrite or delete electronic files. We may also use a third party to safely dispose of records on Pivot's behalf. If we do so, we require the third party to provide sufficient guarantees that it complies with data protection law.

17. Personal data breaches

Pivot will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the Pivot website, which shows the exam results of learners eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a Pivot laptop containing non-encrypted personal data about learners

We will also notify the date subject where we are legally required to do so.

18. Complaints

Data subjects have the right to make a complaint to Pivot if they consider we have not complied with data protection legislation. Any complaints relating to data protection must be directed to our Data Protection Officer.

When dealing with complaints relating to data protection, we shall:

- Acknowledge receipt of the complaint within 30 days of the date on which the complaint is received by Pivot
- Take appropriate steps to respond to the complaint, including making enquiries into the subject matter of the complaint, to the extent appropriate
- Inform the complainant about progress of the complaint
- Inform the complainant of the outcome of the complaint

19. Training

All staff are provided with data protection training as part of their induction process, which is then reviewed and revisited on an annual basis.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

20. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed every six months and approved by the Board of Directors.

21. Links with other policies

This data protection policy is linked to our:

- Data retention policy
- Data protection impact assessment guidance
- Safeguarding policies
- Privacy notices
- AI policy
- Acceptable Use of ICT policy

22. Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

On finding or causing a breach or potential breach, the staff member or data processor must immediately notify the DPO by emailing sarah.howarth@pivot-group.co.uk.

The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people

Staff will co-operate with the investigation (including allowing access to information and responding to questions). This investigation will not be treated as a disciplinary investigation.

If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the headteacher and the COO.

The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g., from IT providers). (See the actions relevant to specific data types at the end of this procedure)

The DPO will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences

The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool

The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored within the designated area on Pivot's secure server.

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of Pivot's awareness of the breach. As required the DPO will set out:

- A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach

- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

If all the above details are not yet known, the DPO will report as much as they can within 72 hours of Pivot's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

Where Pivot is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:

- A description, in clear and plain language, of the nature of the personal data breach
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.

The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts and cause
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored within the designated area on Pivot's secure server.

The DPO and headteacher will meet to review what happened and how it can be prevented in future. This meeting will happen as soon as reasonably possible.

The DPO and headteacher will meet half termly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches.

Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error

- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask Pivot's IT support provider to attempt to recall it from external recipients and remove it from Pivot's email system (retaining a copy if required as evidence)
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it is appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted
- If safeguarding information is compromised, the DPO will inform the Lead Social Worker and Designated Safeguarding Lead and discuss whether Pivot should inform any, or all, of its local safeguarding partners.
- Other types of breach that you might want to consider could include:
    - Details of pupil premium interventions for named children being published on the Pivot website
    - Non-anonymised learner exam results
    - A Pivot laptop containing non-encrypted sensitive personal data being stolen or hacked
    - Hardcopy reports sent to the wrong learners or families