



preparing the way for others to follow

UK GDPR & DATA PROTECTION POLICY

Key document details

Equality Impact Assessment required?	Yes / No
If yes, date of EIA	
Ratified:	Autumn1 24
Approver:	Trust Board
Next review:	Autumn1 25

1. AIMS

Pioneer Educational Trust (Pioneer) and the schools within, aim to ensure that all personal data collected about staff, pupils, parents, governors, 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

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by [The Data Protection, Privacy and Electronic Communications \(Amendments etc\) \(EU Exit\) Regulations 2020](#)
- [Data Protection Act 2018 \(DPA 2018\)](#)

It is based on guidance published by the Information Commissioner's Office (ICO) on the [GDPR](#).

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
Criminal offence data	means information about criminal convictions and other sanctions, penalties or security measures imposed as part of the criminal justice process, allegations of criminal activity and related investigations and proceedings. It also includes information relating to the absence of convictions

term	definition
Processing	Anything 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.
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 of personal data.
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.
personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. THE DATA CONTROLLER

Pioneer processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

Pioneer is registered as a data controller with the ICO as legally required and will renew this registration as legally required.

5. ROLES AND RESPONSIBILITIES

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

5.1 Board of Trustees

Pioneer's Board of Trustees have overall responsibility for ensuring that Pioneer schools comply with all relevant data protection obligations.

The day-to-day responsibility is delegated to the CEO.

5.2 Data Protection Officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will support Pioneer in providing an annual report of their activities directly to the Pioneer Board and, where relevant, report to the Board their advice and recommendations on school data protection issues.

Our DPO is Nicola Cook is Pioneer's DPO and is contactable via blynn@pioneereducationaltrust.org.uk

5.3 Head

The Head will act as the representative of the data controller on a day-to-day basis.

5.4 Staff

Staff are responsible for:

- Collecting, storing and processing all personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Through Pioneer's DPO lead, 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 you have any concerns that this policy is not being followed
 - If you are unsure whether or not Pioneer has a lawful basis to use personal data in a particular way
 - If you 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 suspected data breach
 - Whenever you are engaging in a new activity that may affect the privacy rights of individuals
 - If you need help with any contracts or sharing personal data with third parties

6 DATA PROTECTION PRINCIPLES

The UK GDPR is based on data protection principles that Pioneer must comply with. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

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

7. COLLECTING AND USING PERSONAL DATA

7.1 Lawfulness, fairness and transparency

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

- The data needs to be processed so that Pioneer can fulfil a contract with the individual, or the individual has asked Pioneer to take specific steps before entering into a contract
- The data needs to be processed so that Pioneer 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 Pioneer, as a public authority, can perform a task in the public interest or exercise its official authority
- The data needs to be processed for the legitimate interests of Pioneer (where the processing is not for any tasks Pioneer performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden
- The individual (or their parent/carers when appropriate in the case of a pupil) has freely given clear consent

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

- The individual (or their parent/carers when appropriate in the case of a pupil) 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
- For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law.
- The data needs to be processed to perform or exercise obligations or rights in relation to employment, social security or social protection law
- The individual (or their parent/carers when appropriate in the case of a pupil) 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 including but not limited to safeguarding of children at risk

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law, by issuing the relevant privacy notice, which is also published on our schools' and Pioneer's websites. 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.

You must only use personal data for one of the purposes listed above. You must not use any personal information collected by us for any personal use or for any other purpose than it was collected.

7.2 Relevant, limited and accurate

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.

You must only process personal data to the extent that is necessary in order to do your job.

We will keep data accurate and, where necessary, up-to-date. Inaccurate data will be rectified or erased when appropriate.

In addition, when personal data which you deal with is no longer needed you must ensure it is deleted or anonymised in accordance with Pioneer's record retention schedule.

You must notify the school of any changes to personal data (such as change of a pupil's address or the school's point of contact in relation to a pupil) as a matter of urgency.

7.3 Sharing personal data

Within Pioneer we operate a "need to know" policy which means that you may only share personal information internally with those who need to know it to do their job

We may need to share personal data with entities outside of Pioneer. These circumstances include, but are not limited to, situations where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent if necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
 - Only appoint suppliers or contractors which 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, including for:
 - The prevention or detection of crime and/or fraud
 - The apprehension or prosecution of offenders
 - The assessment or collection of tax owed to HMRC
 - In connection with legal proceedings
 - Where the disclosure is required to satisfy our safeguarding obligations
- We may share personal data to the extent necessary for the purpose of taking legal advice, insurance, audit and accounting.

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 pupils or staff.

You must not share personal data outside of Pioneer for any purpose other than listed above or with the DPO's permission.

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

8 SUBJECT ACCESS REQUESTS AND OTHER RIGHTS OF INDIVIDUALS

8.1 Subject Access Requests

Individuals have a right to make a 'subject access request' to gain access to personal information that Pioneer 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. It's simply a request (whether made verbally or in writing and whether made in a formal letter, an email or even via social media) which asks for details of the information held by Pioneer about an individual. You can ask an individual to complete the form at Appendix 1 but we cannot insist that a subject access request is presented via our form.

If you receive a subject access request in any form you must immediately inform Pioneer's DPO Lead. You must also make a very clear note of any subject access request which you receive verbally including the date on which the request was received. If the individual continues to contact you in relation to their subject access request, please refer them to the DPO.

Once a subject access request has been received, personal data within the scope of the subject access request must not be deleted unless such deletion would have taken place in accordance with Pioneer's record retention schedule. You must therefore not delete any information relating to an individual who has submitted a subject access request unless you have the DPO's permission to do so.

8.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. So long as a child is competent to exercise their data protection rights, they can submit a subject access request themselves. 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 for their parent to act on their behalf.

In England there is no set age at which a child is considered to have competency which is assessed depending on the understanding of the child. However, as a starting point, many children who are 12 or older will usually have the necessary level of understanding while those who are younger will often not. Therefore, most subject access requests relating to Pioneer's pupils will most likely be submitted by the

parent or carer. The DPO will assess if the child has sufficient understanding of their rights to allow Pioneer to provide the personal data to the parent or carer without the pupil's authorization to do so.

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 without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- 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 pupil 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.

8.3 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
- 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 which 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

Individuals should submit any request to exercise these rights to the DPO. If you receive such a request, you must immediately seek advice from the DPO Lead.

8.4 Parental requests to see the educational record

For Academies, there is no automatic parental right of access to the educational record of their child as there is for pupils in maintained schools.

However, Pioneer will aim to follow the requirements imposed on maintained schools and provide the educational record to parents, or those with parental responsibility, within 15 school days of receipt of a written request so long as the pupil concerned does not object to the provision of their educational record to their parent/person with parental responsibility or the pupil does not have capacity to exercise their data protection rights.

If the request is for a copy of the educational record, the school will charge a fee to cover the cost of supplying it.

Pioneer will not provide copies of an educational record to parents of a pupil aged 18 or older. There are certain circumstances in which such a request will be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

9. BIOMETRIC RECOGNITION SYSTEMS

Please refer to our 's Protection of Children's Biometric Information Policy

10. CCTV

Please refer to our CCTV policy.

11. PHOTOGRAPHS AND VIDEOS

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

For children of primary school age, 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 pupil.

For children of secondary school age, we will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Any photographs and videos taken by parents/carers (of children of any age) at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or

videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.

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.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to seek to reduce them being identified.

12. DATA PROTECTION BY DESIGN AND DEFAULT

Protecting privacy and personal information is not a stand-alone exercise nor should it be an afterthought when designing and implementing new projects. In fact, we are required to put in place what is called “Privacy by Design” i.e. an approach to projects that promotes privacy and data protection compliance from the start.

We have the following measures in place to show that we have integrated data protection into all of our data processing activities:

- Appointed a suitably qualified independent DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only process 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)
- Complete data protection impact assessments where the 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)
- Regularly train staff on data protection law, this policy, any related policies and any other data protection matters
- Regularly conduct reviews and audits to test our privacy measures and make sure we are compliant

12.1 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.

You must follow the following rules.

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, must be 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
- Hard copy documents should not be taken off Pioneer premises unless you have your manager’s permission to do so;
- Where you remove any personal data from Pioneer’s premises you are responsible for keeping it secure and preventing access by any third party, including members of your family or visitors to your home.
- Hard copy documents and electronic devices including laptops and mobile phones which have access to Pioneer’s systems or on which personal data is stored must not be left in an unattended vehicle;

- Personal data whether stored on a laptop or printed on a document must not be read in public places such as on public transport.
- Hard copy documents should not be transported in clear or partially transparent folders.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- You must not download software to an electronic device used by you for work purposes without permission of the Head/CEO
- You must use your best efforts to prevent any portable devices and removable media being lost or stolen
- When you are not using an electronic device, including any time you step away from your workstation, you must turn it off or lock the screen.
- You must use a pin or password to protect all electronic devices and not share these with anyone else. You should not use the same pin for various devices. If a pin or password is compromised, you must change it immediately.
- You must not allow anyone who is not a Pioneer employee to use any electronic device provided to you by Pioneer
- You must not seek to remove any anti-virus or anti-malware software from any electronic devices which you use for work purposes;
- You must not back up any information locally or to a cloud-based storage which is not used by Pioneer.
- You must not use public wi-fi when accessing any personal data processed by Pioneer on any device
- You must not use any device to capture images, video or audio within the workplace (whether using facilities native to the device or through third party applications).

To ensure the security of personal data processed by Pioneer we reserve the right to inspect any devices for unauthorized use or for breach of this policy. You must co-operate with us to enable such inspection, access and review, including providing any passwords or pin numbers necessary to access the device or relevant applications. A failure to co-operate with us in this way may result in disciplinary action being taken, up to and including dismissal without notice.

In the event that your device is lost or stolen or where you believe that a device may have been accessed by an unauthorised person or otherwise compromised, you must report the incident to our IT Department and the DPO lead immediately. You must co-operate with Pioneer in taking appropriate steps to ensure that school information (including personal data) on or accessible from the device is secured, including remote wiping of the device where appropriate. The remote wipe will destroy all information belonging to Pioneer, including personal data, on the device (including information contained in a work e-mail account) and may inadvertently destroy your personal information.

If we discover or reasonably suspect that there has been a breach of this policy, including any of the security requirements listed above, we may immediately remove access to our systems and, where appropriate, remove any school information (including personal data) from your device. Although we do not intend to wipe other information that is personal to you (such as photographs or personal files or e-mails), it may not be possible to distinguish all such information from school information in all circumstances. You should therefore regularly backup any information which is personal to you contained on the device.

12.2 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 Pioneer's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

12.3 Personal data breaches

Pioneer will make all reasonable endeavours to ensure that there are no personal data breaches. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, and can occur if personal data has been accidentally or unlawfully, lost, stolen, destroyed, altered, disclosed or made available where it should not have been or made available to unauthorised people. Examples of potential data breaches include:

- Loss of a device eg laptop, mobile on which personal data is stored;
- Sending an email to the wrong recipient
- Sending personal data to your personal email account rather than your work account

In the event of a suspected data breach, you must report the incident to the DPO immediately. Do not seek to investigate the matter yourself, do not destroy any records or attempt to cover up any actions. We will follow the procedure set out in appendix 2.

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it.

13. TRAINING

All staff are provided with data protection training which is refreshed on a two-year cycle. Data protection will also form part of continuing professional development, where changes to legislation, guidance or Pioneer's processes make it necessary.

Appendix 1

Subject Access Request Form

If you would like us to supply you with a copy of any personal data we hold about you, you are encouraged to submit your request by completing this form. You are entitled to receive this information under the Data Protection Act 2018 (DPA) and UK General Data Protection Regulation (GDPR). We will also provide you with information about any processing of your personal data that is being carried out, the retention periods which apply to your personal data, and any rights to rectification, erasure, or restriction of processing that may exist.

We will endeavour to respond promptly and usually within one month of the latest of the following:

- Our receipt of your written request; or
- Our receipt of any further information we may ask you to provide to enable us to comply with your request.

The information you supply in this form will only be used for the purposes of identifying the personal data you are requesting and responding to your request.

SECTION 1: Details of the person requesting information

Full name:	
Address:	
Contact telephone number:	
Email address:	

SECTION 2: Are you the data subject i.e. the person who the data is about?

Please tick the appropriate box and read the instructions which follow it.

- ☐ YES: I am the data subject. I enclose proof of my identity (see below) or I am a member of staff submitting this form from my work email address.
(please go to section 4)
- ☐ NO: I am acting on behalf of the data subject. I have enclosed the data subject's written authority and proof of the data subject's identity and my own identity (see below).
(please go to section 3)

To ensure we are releasing data to the right person we require you to provide us with proof of your identity and of your address. Please supply us with a photocopy or scanned image (do not send the originals) of one of both of the following:

1) Proof of Identity

Passport, photo driving licence, national identity card, birth certificate.

2) Proof of Address

Utility bill, bank statement, credit card statement (no more than 3 months old); current driving licence; current TV licence; local authority tax bill, HMRC tax document (no more than 1 year old).

If we are not satisfied you are who you claim to be, we reserve the right to refuse to grant your request.

SECTION 3: Details of the data subject (if different from section 1)

Full name:	
School:	
Address:	
Contact telephone number:	
Email address:	
Age	
Does the data subject consent to you acting on their behalf?	
If not, what is your relationship to the data subject?	

SECTION 4: What information are you seeking?

Please describe the information you are seeking. Please provide any relevant details you think will help us to identify the information you require.

--

Please note that if the information you request reveals details directly or indirectly about another person, we have to comply with our duty to protect their data. We will assess if their data can be redacted or it is appropriate to seek their consent and if not whether it is nonetheless appropriate to reveal their data to you. In certain circumstances, where disclosure would adversely affect the rights and freedoms of others, we may not be able to disclose the information to you, in which case you will be informed promptly and given reasons for that decision. There are other grounds on which we may not disclose data to you, if these apply we will explain them in our response to you.

While in most cases we will be happy to provide you with copies of the information you request, we nevertheless reserve the right, , not to provide you with copies of information requested if to do so would take “disproportionate effort”, to charge a fee or refuse the request if it is considered to be “manifestly unfounded or excessive”. However, we will make every effort to provide you with a satisfactory form of access or summary of information if suitable.

SECTION 5: Declaration

Please note that any attempt to mislead may result in prosecution.

I confirm that I have read and understood the terms of this subject access form and certify that the information given in this application to Pioneer Educational Trust is true.

I understand that it is necessary for Pioneer Educational Trust to confirm my / the data subject’s identity and it may be necessary to obtain more detailed information in order to locate the correct personal data.

Please delete where not applicable, the data subject is my child and gives their consent to you releasing the above requested data to me. We understand that Pioneer will need to undertake its own assessment as to my child’s capacity to exercise their data protection rights and the DPO is likely to need to talk to my child before deciding how to respond to this request.

Signed..... Date
Data Subject

Signed..... Date
Person acting on behalf of the data subject

Documents which must accompany this application:

- Evidence of your identity (see section 2)

- Evidence of the data subject's identity (if different from above)
- Authorisation from the data subject to act on their behalf (if applicable)

Please return the completed form to the DPO.

Correcting Information

If after you have received the information you have requested you believe that:

- Any information is inaccurate or out of date; or
- we should no longer be holding that information; or
- we are using your information for a purpose of which you were unaware;
- we may have passed inaccurate information about you to someone else;

Then you should notify the DPO at once.

Appendix 2: Personal data breach procedure

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

- A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, and can occur if 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
- On finding or causing a personal data breach, or potential personal data breach, in relation to personal data for which Pioneer is responsible, the staff member, governor or data processor must immediately notify the DPO.
- The DPO will investigate the report, and determine whether a breach has occurred.
- Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation, although it may lead to a disciplinary investigation
- If a personal data breach has occurred or it is considered to be likely that is the case, in the opinion of the DPO, the DPO will alert the CEO and Head
- The DPO will advise on all reasonable efforts to contain and minimise the impact of the personal data breach. Relevant staff members or data processors will help with this where necessary
- 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 personal data breach must be reported to the ICO and the individuals affected using the ICO's [self-assessment tool](#)
- The DPO Lead 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 personal data breach.
- Where the ICO must be notified, the DPO will do within 72 hours of the school's awareness of the personal data 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 personal data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will also provide any further or updated relevant information to the ICO, as such information comes to light
- 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 investigate the personal data breach, mitigate Pioneer's potential liability and/or mitigate the loss to individuals – for example, the police, insurers, external legal counsel, IT and forensic investigators, banks and credit card companies

- Each personal data breach will be documented by the DPO, 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)