Pathfinder
Multi Academy Trust

DATA AND INFORMATION GOVERNANCE:

# Data Protection Policy

This policy has been adopted by Pathfinder Multi Academy Trust and is applicable across all schools that make up the Trust. In line with the MAT's Scheme of Delegation, this Policy must be duly applied by each Local Governing Committee and the Headteacher of each school in Pathfinder Multi Academy Trust.

Where there are specific details or any discretions in the policy that apply to an individual school or Local Governing Committee this has been made clear within the wording of the policy.

This policy will be reviewed in line with the agreed timetable for policy review or sooner as events or legislation changes require.

Date Adopted: October 2026

Date for Review: October 2027

2026-27 changes to this policy:

**Section 11. Data Protection Complaints** - additional information relating to the complaints procedures

**Appendix 6 - Biometrics** - Added section ‘ Bias and/or discrimination’

# Contents

1 Introduction and Scope 4
2 Roles and Responsibilities 4
3 Data Protection Principles 5
4 Lawful Bases 6
5 Data Subject Rights 6
6 Records of Processing 7
7 Privacy by Design and Risk Assessments 7
8 Information Sharing 7
9 Contract Management 8
10 Training 8
11 Data Protection Complaints 8
Appendix 1 - Appropriate Policy Document (APD) 10
Appendix 2 - Subject Access Requests (SAR) 13
Appendix 3 - Freedom of Information (FOI) and Environmental Information Regulation (EIR) Requests 15
Appendix 4 - Surveillance 18
Appendix 5 - Surveillance Camera System Checklist 21
Appendix 6 - Biometrics 23

# 1 Introduction and Scope

Pathfinder Multi Academy Trust is required to process personal information about staff, students, parents, carers and other individuals we may interact with. We must do this in compliance with data protection and other relevant legislation.

This policy provides a framework for ensuring that we comply with the requirements of the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018 (DPA), and other relevant legislation, as well as associated guidance and codes of practice.

This policy including its appendices applies to our entire workforce. This includes employees, governors or Trustees, contractors, agents and representatives, volunteers and temporary staff working for, or on behalf of, the school. Individuals who are found to knowingly or recklessly infringe this policy may face disciplinary action.

This policy is the Trust's main information governance policy and applies to all personal data, regardless of whether it is in paper or electronic format.

Information security, data breaches, acceptable use of systems and records management are addressed in separate policies.

# 2 Roles and Responsibilities

Overall responsibility for ensuring that the Trust meets the statutory requirements of any data protection legislation lies with the trustees. The following roles have day to day responsibility for compliance and provide the necessary assurance to the Board.

### Data Protection Officer (DPO)

The role of the DPO is to assist the school in monitoring compliance with the UK GDPR and the Data Protection Act 2018 and advise on data protection issues. We have appointed Veritau as our DPO. Veritau's contact details are:

Schools Data Protection Officer
Veritau
West Offices
Station Rise
York
North Yorkshire
YO1 6GA

schoolsDPO@veritau.co.uk // 01904 554025

The DPO is an advisory role, and its duties include:

- Informing and advising us and our employees about our obligations to comply with UK GDPR and other data protection laws,
- Monitoring compliance with data protection legislation and internal policies,
- Raising awareness of data protection issues and conducting compliance reviews, and
- Liaising with the Information Commissioners Office (ICO).

### Senior Information Risk Owner

The SIRO is a senior member of staff who has ultimate responsibility for operational risk, ensuring that the Trust's policies and procedures are effective and comply with legislation, and promoting good practice in school. In our organisation this role lies with the Chief Operating Officer.

### Single Point of Contact (SPOC)

The SPOC is someone at school level who can take operational responsibility for data protection, including communicating with data subjects and the DPO. In our organisation this role lies with the Compliance Officer at Trust Level and School Business Managers in individual schools.

### Information Asset Owner (IAO)

An IAO is an individual who is responsible for the security and maintenance of a particular information asset. They are responsible for ensuring that other members of staff are using the information safely and responsibly. We will ensure that IAO's are appointed based on sufficient seniority and level of responsibility, and document this in our Information Asset Register (IAR).

### All staff

All staff, including governors or trustees, contractors, agents and representatives, volunteers and temporary staff working for, or on behalf of, the school are responsible for collecting, storing and processing any personal data in accordance with this policy.

## 3 Data Protection Principles

We will comply with the data protection principles, as defined in Article 5 of the UK GDPR. We will ensure that personal information is:

- Processed lawfully, fairly and in a transparent manner (**Lawfulness, Fairness and Transparency**).
- Collected only for specified, explicit and legitimate purposes (**Purpose Limitation**).
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (**Data Minimisation**).
- Accurate and where necessary kept up to date (**Accuracy**).
- Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed (**Storage Limitation**).
- Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (**Security, Integrity and Confidentiality**).

We recognise that not only must we comply with the above principles, we must also demonstrate our compliance (**Accountability**).

# 4 Lawful Bases

UK GDPR sets out several conditions under which we can process personal information lawfully. We usually rely on the lawful basis of Public Task or Legal Obligation, however at times we may rely on our legitimate interests. We will only do this where we are using data in ways individuals would reasonably expect and where we have a justifiable reason.

When relying on our legitimate interests, we will ensure that we provide individuals with clear and transparent information about how personal data will be used, including details on how to opt-out.

We may rely on vital interests as the lawful basis for sharing information in a situation where we believe someone is at risk of serious harm, for example, in a mental health emergency.

We have an Appropriate Policy Document (APD) in place (see Appendix One) which provides information about our processing of special category (SC) and criminal offence (CO) data. The APD demonstrates how we comply with the requirements of the UK GDPR and DPA.

# 5 Data Subject Rights

Under the UK GDPR, individuals have several rights in relation to the processing of their personal data:

### Right to be informed

We provide individuals with privacy information at the time we collect their data, normally by means of a privacy notice, which is made easily accessible to the data subject. Privacy notices will be clear and transparent, regularly reviewed, and include all information required by data protection legislation.

### Right of access

Individuals have the right to access and receive a copy of the information we hold about them. This is commonly known as a subject access request (SAR). We have in place a SAR procedure which details how we deal with these requests (Appendix Two).

Other rights include the right to rectification, right to erasure, right to restrict processing, right to object, right to data portability and rights related to automated decision-making, including profiling.

Requests exercising these rights can be made to any member of staff, but we encourage requests to be made in writing, wherever possible, and forwarded to the school's Headteacher or School Business Manager who will acknowledge the request and respond within one calendar month. Advice regarding such requests will be sought from our DPO where necessary.

A record of decisions made in respect of the request will be retained, recording details of the request, whether any information has been changed, and the reasoning for the decision made.

# 6 Records of Processing

In accordance with Article 30 of UK GDPR, we must keep a record of our processing activities. We will do this by developing and maintaining an Information Asset Register (IAR) which will include as a minimum:

- The school or Trust's name and contact details
- The name of the information asset
- The owner of that asset, known as the Information Asset Owner (IAO)
- The purposes of the processing
- A description of the categories of individuals and the types of personal data
- Who has access to the personal data, and who it is shared with
- The lawful bases for each processing activity
- The format and location of the personal data
- Details of any transfers to countries outside of the UK, and the appropriate safeguards
- The retention periods for each asset
- A general description of the technical and organisational security measures to protect the information.

We will review the IAR at least annually to ensure it remains accurate and up to date, consulting with the DPO as necessary.

# 7 Privacy by Design and Risk Assessments

We will adopt a privacy by design approach and implement appropriate technical and organisational security measures to demonstrate how we integrate data protection into our processing activities.

We will conduct a data protection impact assessment (DPIA) when undertaking new, high-risk processing, or making significant changes to existing data processing. The purpose of the DPIA is to consider and document the risks associated with a project prior to its implementation, ensuring data protection is embedded by design and default.

All of the data protection principles will be assessed to identify specific risks. These risks will be evaluated and solutions to mitigate or eliminate these risks will be considered. Where a less privacy-intrusive alternative is available, or the project can go ahead without the use of special category data, we will opt to do this.

# 8 Information Sharing

In order to efficiently fulfil our duty of education provision it is sometimes necessary for us to share information with third parties. Routine and regular information sharing arrangements will be documented in our privacy notices and in our IAR.

Any further or ad-hoc sharing of information will only be done so in compliance with legislative requirements, including the ICO's data sharing code of practice. We will only share personal information where we have a lawful basis to do so, ensuring any disclosure is necessary and proportionate. All disclosures will be approved by the relevant staff member and recorded in a disclosure log.

# 9 Contract Management

All third-party contractors who process data on our behalf must be able to provide assurances that they have adequate data protection controls in place. Where personal data is being processed, we will ensure that there is a written contract in place which includes all the mandatory data processing clauses, in accordance with Article 28 of the UK GDPR.

We will maintain a record of our data processors, and regularly review the data processing contracts, with support from the DPO, to ensure continued compliance.

### International Transfers

Where possible, personal information we process is not transferred outside of the European Economic Area (EEA), which the UK government deems to have adequate data protection standards. If personal data is transferred outside the EEA, we will consult with the DPO and take reasonable steps to ensure appropriate safeguards are in place. These safeguards will be recorded in our data processor register.

# 10 Training

We will ensure that appropriate guidance and training is given to our workforce, governors or trustees, and other authorised school users on data protection and access to information. Training will be delivered as part of the induction process and at least every two years. Refresher training will be carried out at appropriate intervals.

Specialised roles or functions with key data protection responsibilities, such as the SIRO, SPOC and IAOs, will also receive additional training specific to their role.

We will maintain a record of all training that has been completed and ensure that data protection awareness is raised in staff briefings and as standard agenda items in meetings, where appropriate.

# 11 Data Protection Complaints

Data protection complaints relating to a completed SAR will be processed as an internal review request in accordance with Appendix 2.

Any other complaints or concerns about our compliance with data protection legislation or our handling of personal data will be dealt with as a data protection complaint.

Our general data protection complaints procedure is as follows:

- Complaints may be received directly by email, telephone, or in person. Alternatively, individuals may contact our Data Protection Officer.
- We encourage individuals to provide sufficient evidence or supporting information where possible, to allow us to investigate the complaint.
- If necessary, we may request proof of ID (or proof of authority where the complainant is acting on behalf of another person).
- We will acknowledge complaints within 30 days of receipt. This includes weekends and bank holidays.

- We will take steps to respond to complaints without undue delay. This includes making appropriate enquiries and keeping the complainant informed.
- We will inform people of the outcome of their complaints. This includes explaining any steps we have taken to address the complaint.

If an individual remains dissatisfied after we have concluded our internal data protection complaints process, they may complain to the Information Commissioner's Office. Its contact details are below:

The telephone helpline (0303 123 1113) is open Monday to Friday between 9 a.m. and 5 p.m. (excluding bank holidays). Alternative methods for reporting, enquiring, registering, and raising complaints are available on the ICO's website here.

# Appendix 1 - Appropriate Policy Document (APD)

## Introduction

Pathfinder Multi Academy Trust processes special category and criminal conviction data in the course of fulfilling its functions as a Trust. Schedule 1 of the Data Protection Act 2018 requires data controllers to have in place an 'appropriate policy document' where certain processing conditions apply for the processing of special categories of personal data and criminal convictions data. This policy fulfils this requirement.

This policy complements our existing records of processing as required by Article 30 of UK General Data Protection Regulation. It also reinforces our existing retention and security policies, procedures and other documentation in relation to special category data.

## Special categories and conditions of processing

We process the following special categories (SC) of data:

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade union membership,
- health,
- sex life/orientation,
- biometric identifiers.

We also process criminal offence (CO) data under Article 10 of UK GDPR, including for pre-employment checks and declarations by employees in line with their contractual obligations.

We rely on the following processing conditions under Article 9 of UK GDPR and Schedule 1 of the Data Protection Act 2018 to lawfully process special category and criminal convictions data:

**Article 9(2)(a) - explicit consent**
We will ensure that consent obtained from individuals is clear and specific for one or more outlined purposes. It must be granted through affirmative action and recorded as a requirement for processing. We will also conduct regular reviews of consents to ensure they remain current and valid.

Examples of such processing include when we use biometric (fingerprint) data for identification or authentication purposes for school meal payments; or when we ask for health or medical information from visitors to aid them in the event of an emergency.

**Article 9(2)(b) - employment, social security or social protection**
To comply with our legal requirements as an employer and safeguard our pupils, we need to collect some special category data.

Examples include when we carry out DBS checks on staff to evidence suitability for a role; collect medical information to put in reasonable adjustments at work and monitor staff absence; and keep records of an employee's trade union membership.

When processing information under Article 9(2)(b), we also require a Schedule 1 condition under the Data Protection Act 2018. The condition we rely on for this processing is **Schedule 1, Part 1, (1) - employment, social security and social protection**.

**Article 9(2)(c) – vital interest**
We must share SC data where an individual is physically or legally unable to consent and there is a serious risk to life.
An example is when there is an urgent or emergency situation, and an individual is at risk of harm to themselves or to others, such as in a mental health crisis.
A Schedule 1 condition is not required for processing under Article 9(2)(c).

**Article 9(2)(g) - reasons of substantial public interest**
We have a wide variety of duties we must carry out in the public interest. Much of our processing of SC data is done so for the purposes of substantial public interest.

Examples include when we process SC data to identify students who require additional support such as special educational needs; processing safeguarding concerns to ensure the safety and wellbeing of pupils; or collecting medical information when monitoring pupil attendance or dietary requirements.

When processing data under Article 9(2)(g), we also require a Schedule 1 condition under the Data Protection Act 2018. The conditions we rely on for this processing are **Schedule 1, Part 2, (6) - statutory and government purposes; (10) - preventing or detecting unlawful acts; and (18) - safeguarding of children and of individuals at risk.**

## Compliance with Data Protection Principles

We have several policies and procedures in place to ensure our compliance with the Article 5 Data Protection Principles and meet our accountability obligations, explained in more detail below:

**Accountability principle**
We have put in place appropriate technical and organisational security measures to meet the requirements of accountability. These include:

- The appointment of a Data Protection Officer, Veritau.
- Taking a data protection by design and default approach to our processing activities, including the use of risk assessments.
- Maintaining documentation of our processing activities through an Information Asset Register.
- Adopting and implementing an information governance framework
- Ensuring we have compliant contracts in place with data processors.
- Implementing appropriate security measures in relation to the personal data we process. More detail can be found in our Information Security Policy.

**Principle (a): lawfulness, fairness and transparency**
Processing personal data must be lawful, fair and transparent. We have identified an appropriate Article 6 condition and also, where processing SC or CO data, an Article 9 and Schedule 1 condition.

We consider how any processing may affect individuals concerned and provide clear and transparent information about why we process personal data, including our lawful bases, in our privacy notices and this policy document. All privacy notices provide details of data subject rights. Our privacy information is regularly reviewed and updated to ensure it accurately reflects our processing.

**Principle (b): purpose limitation**
Organisations can only act in ways and for purposes which they are empowered to do so by law. Personal data is therefore only processed to allow us to carry out the necessary functions and services we are required to provide in line with legislation. We clearly set out our purposes for processing in our privacy notices, policies and procedures, and in our IAR. If

we plan to use personal data for a new purpose, other than a legal obligation or function set out in law, we check that it is compatible with our original purpose, or we advise individuals of the new purpose.

**Principle (c): data minimisation**
We only collect the minimum personal data needed for the relevant purposes, ensuring it is necessary and proportionate. Any personal information that is no longer required, especially where it contains special category data, is anonymised or erased. Further information can be found in our Records Management Policy.

**Principle (d): accuracy**
When we become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is processed, we will take every reasonable step to ensure that data is erased or rectified without delay. Where we are unable to erase or rectify the data, for example because the lawful basis we rely on to process the data means these rights do not apply, we will document our decision.

Where we have shared information with a third party, we will take all reasonable steps to inform them of the inaccuracies and rectification. We maintain a log of all data rights requests and have appropriate processes for handling such requests.

**Principle (e): storage limitation**
We have a Retention Schedule in place which is based on guidance issued by the Information and Records Management Society (IRMS). This sets out how long we retain records. Where there is no legislative or best practice guidance in place, the SIRO will decide how long the information should be retained based on its necessity for legitimate purposes. We also maintain a Destruction Log, which documents what information has been destroyed, the date it was destroyed and why it has been destroyed. Further information can be found in our Records Management Policy.

**Principle (f): integrity and confidentiality (security)**
We employ various technical and organisational security measures to protect the personal and special category data that we process. A full description of security measures can be found in our Information Security Policy.

In the event of a personal data breach the incident will be recorded in a log, investigated, and reported to our Data Protection Officer where necessary. High risk incidents are reported to the Information Commissioner's Office. This process is documented in greater detail in our Information Security Policy.

# Appendix 2 - Subject Access Requests (SAR)

Under the UK GDPR, individuals have the right to make a subject access request (SAR) to any member of our workforce, governor or trustee, or contractor or agent working for the school. Requests need not be made in writing, but we encourage applicants to do so where possible. Requests should be forwarded to the school's Headteacher or School Business Manager who will log the request and acknowledge it within five school days.

We must be satisfied of the requestor's identity and may have to ask for additional information to verify this, such as:

- valid photo ID, such as driver's licence or passport,
- proof of address, such as a utility bill or council tax letter, or
- confirmation of email address.

Only once we are confident of the requestor's identity and have sufficient information to understand the request will it be considered valid. We will then respond to the request within the statutory timescale of one calendar month.

We can apply a discretionary extension of up to a further two calendar months to comply if the requested information is considered 'complex'. If we wish to apply an extension, we will firstly seek guidance from our DPO, then inform the applicant of the extension within the first calendar month of receiving the request.

Requests are considered 'complex' only if we can demonstrate that they meet one or more of the following factors:

- Information is technically difficult to retrieve, or specialist support is required.
- Large volumes of sensitive information where exemptions may need to be applied.
- Clarifying potential issues concerning confidentiality and/or disclosure of sensitive information.
- Needing to obtain specialist legal advice.
- Searching large volumes of unstructured manual records.

Requests involving large volumes of information may add complexity, but volume alone is not considered 'complex.'

If we think it necessary to apply any exemptions to the requested information before disclosure, we will seek guidance from our DPO. In limited circumstances, we may also refuse a request on the basis that it is manifestly unreasonable or excessive.

If a subject access request is made by a parent whose child is 12 years of age or over, we may consult with the child or ask that they submit the request on their own behalf or confirm permission for the request. This decision will be made based on the capacity of the pupil in question.

### Internal Review

Complaints in relation to SARs will be processed as an internal review request. When acknowledging receipt, we will inform you that we are processing your complaint as an internal review request.

An internal review will be dealt with by an appropriate member of staff who was not involved in the original request. They will examine the original request and response and decide whether it was dealt with appropriately under the legislation. The reviewing officer will decide whether to uphold or overturn any exemptions. A full response will be provided within one calendar month where possible.

If an individual remains dissatisfied after we have concluded our investigation, they may appeal to the Information Commissioner's Office. Their contact details are below:

The telephone helpline (0303 123 1113) is open Monday to Friday between 9 a.m. and 5 p.m. (excluding bank holidays). Alternative methods for reporting, enquiring, registering, and raising complaints are available on the ICO's website here.

# Appendix 3 - Freedom of Information (FOI) and Environmental Information Regulation (EIR) Requests

## Freedom of Information (FOI)

The Freedom of Information Act 2000 (FOIA) is part of the Government's commitment to greater openness and transparency in the public sector. It enables members of the public to scrutinise the decisions of public authorities more closely and ensure that services are delivered properly and efficiently. Schools have two main responsibilities under the Freedom of Information Act:

- To publish certain information about its activities in a publication scheme, and
- To process and respond to individual requests for information, with a duty to provide advice and assistance.

Under FOI, anyone can request access to general recorded information we hold. Recorded information includes printed documents, computer files, letters, emails, photographs, and sound or video recordings. A Code of Practice under section 45 of the Act sets out recommendations for the handling of requests for information. To comply with this Code requests must:

- Be in writing,
- Provide the name or company name and contact address or email address,
- Describe the information they are requesting,
- Ideally, state the preferred format they would like the information to be provided.

Any request that cannot be answered promptly as part of normal day to day business or where we are asked to handle it under Freedom of Information, will be treated as a FOI request.

Information can be withheld if one or more of the 24 exemptions within the FOIA apply. This could mean that certain information is not released in response to a request or is not published. Requests for information can be refused for reasons including:

- The information is not held
- It would cost too much or take too much staff time to comply with the request
- The request is considered vexatious
- The request repeats a previous request from the same person

## Environmental Information Regulations (EIR)

Requests for information that relates to the environment, including activities which may affect the environment, are dealt with under the Environmental Information Regulations 2004. EIR is similar to FOI but there is an even greater presumption of disclosure, and there are fewer exceptions under which a request can be refused. Requests under EIR can also be given verbally and do not need to be in writing, but must include:

- A name or company name and contact address or email address,
- A description of the information being requested,
- Ideally, the preferred format they would like the information to be provided.

"Environmental Information" includes information which relates to:

a) the state of the elements of the environment, such as air and atmosphere, water, soil, land, landscape and natural sites including wetlands, coastal and

marine areas, biological diversity and its components, including genetically modified organisms, and the interaction among these elements,

b) factors such as substances, energy, noise, radiation or waste, including radioactive waste, emissions, discharges and other releases into the environment, affecting or likely to affect the elements of the environment referred to in (a),
c) measures (including administrative measures), such as policies, legislation, plans, programmes, environmental agreements, and activities affecting or likely to affect the elements and factors referred to in (a) and (b) as well as measures or activities designed to protect those elements,
d) reports on the implementation of environmental legislation,
e) cost-benefit and other economic analyses and assumptions used within the framework of the measures and activities referred to in (c), and
f) the state of human health and safety, including the contamination of the food chain, where relevant, conditions of human life, cultural sites and built structures in as much as they are, or may be affected by the state of the elements of the environment referred to in (a) or, through those elements, by any of the matters referred to in (b) and (c).

### Requests for information under FOI and EIR

Any requests received should be forwarded to the school's Headteacher or School Business Manager who will log the request and acknowledge within five school days.

The Headteacher or School Business Manager is responsible for:

- Deciding whether the requested information is held,
- Locating, retrieving or extracting the information,
- Considering whether any exemption or exception might apply, and the balance of the public interest test,
- Preparing the material for disclosure and drafting the response,
- Seeking any necessary approval for the response, and
- Sending the response to the requester.

FOI requests must be made in writing. We will only consider requests which provide a valid name and address and we will not consider requests which ask us to click on electronic links. EIR requests can be made verbally, however we will endeavour to follow this up in writing with the requestor to ensure accuracy.

The Trust's Chief Operating Officer and Headteacher will jointly consider all requests where a public interest test is applied or where there is any doubt on whether an exemption should be applied. In applying the public interest test they will:

- Document clearly the benefits of both disclosing or withholding the requested information
- Where necessary, seek guidance from the DPO and previous case law to decide where the balance lies.

Reasons for disclosing or not disclosing will be reported to the next board or committee meeting.

We have adopted the Information Commissioner's model publication scheme for schools and will publish as much information as possible on our website in the interests of transparency and accountability.

We will charge for supplying information at our discretion, in line with current regulations. If a charge applies, written notice will be given to the applicant and payment must be received before the information is supplied.

We will respond to requests within the statutory timeframes of 20 school days for FOI requests and 20 working days for EIR requests.

### Internal Reviews

Complaints in relation to FOI and EIR will be processed as an internal review request and should be made within 40 working days from the applicant receiving the original response. After that time, we are not obliged to respond to the request for a review.

An internal review will be dealt with by an appropriate member of staff who did not have any involvement in the original request. They will examine the original request and the response that was sent and decide whether it was dealt with appropriately, according to legislative requirements. The reviewing officer will also decide whether to uphold or overturn the decisions to withhold information. A full response will be provided within 20 school days.

If an individual remains dissatisfied after we have concluded our internal review they may appeal to the Information Commissioner's Office. Their contact details are below:

Phone: 0303 123 1113 or via their live chat. Their normal opening hours are Monday to Friday between 9am and 5pm (excluding bank holidays). You can also report, enquire, register and raise complaints with the ICO using their web form on Contact us | ICO.

# Appendix 4 - Surveillance

## Introduction

This policy concerns our use of surveillance technology and related processing of personal data. It is written in accordance with data protection and human rights legislation, statutory guidance and relevant codes of practice.

## Definition of surveillance

Surveillance is the close observation or monitoring of people's activities either by physical means, such as surveillance camera systems, or by the collection and analysis of personal data, such as monitoring emails, phone calls, and internet browsing. We only use surveillance in the context of CCTV and e-monitoring software. We do not operate call recording or covert surveillance technologies and therefore this policy does not cover the use of such technology.

## Surveillance cameral systems

A surveillance camera system, formally called CCTV, includes the cameras and all the related hardware and software for transmitting, processing, and storing the captured data. We will operate surveillance camera systems to:

- Protect school buildings and property
- Protect the safety and wellbeing of pupils, our workforce and visitors
- Deter and discourage anti-social behaviour such as bullying, theft and vandalism
- Monitor compliance with school rules and policies
- Support the police in the prevention, detection, investigation and prosecution of any crimes.

## E-monitoring

'E-monitoring' or 'digital monitoring' is when an organisation uses software to monitor a user's activity on an electronic device or network. We will deploy e-monitoring software across our network, covering fixed and portable devices (PCs, laptops, and tablets), including guest devices connected to our network.

The software will monitor typed activity and the content visible on a user's screen to detect inappropriate use. Inappropriate use will be reported to designated staff within our organisation through a screenshot and other relevant technical details for further investigation. Staff, students and guests accessing our network are subject to this monitoring.

We operate e-safety monitoring software systems to:

- Safeguard our pupils and staff
- Promote wellbeing and early intervention
- Ensure appropriate use of school assets and resources
- Monitor compliance with school rules and policies

The Trust uses Smoothwall and NYNET for e-monitoring purposes.

## Data protection by design and default

Under the UK GDPR, we are required to consider and address privacy implications to data subjects when implementing new data processing systems. This is known as privacy by

design.  The usual method for assessing privacy risks to individuals is by carrying out a Data Protection Impact Assessment (DPIA).

A DPIA is mandatory for surveillance activities since they are deemed particularly intrusive. We will ensure that DPIAs have been completed for both CCTV and e-monitoring and that there are no unmitigated high risks to the rights and freedoms of data subjects. In addition, we will review and update the relevant DPIA if we substantively change our systems.

We are open and transparent about using surveillance technology and identify whether we are a controller or joint controller of the information. Where we use external providers to process the data on our behalf, we will have a written contract meeting the requirements of Article 28 of the UK GDPR. We will only use providers who can ensure they have appropriate measures to safeguard the data.

### Transparency

The use of surveillance camera systems must be visibly signed. Signage will include the purpose of the system, the name of the organisation operating the system and details of who to contact about its use. The signage will be clear and unobstructed so that anyone entering the area knows they are being recorded.

Users will be informed of e-monitoring in relevant policies, newsletters, internal communications, and visual cues such as notifications on computer log-in screens and/or on the browser page when they join the network.

Our privacy notices will include more detailed information about our use of surveillance technologies, including information about data subject rights.

### Access Controls

Surveillance system data will only be accessed to comply with the specified purpose. For example, footage of camera systems intended to prevent and detect crime will only be examined where there is evidence to suggest criminal activity has occurred. Logs of e-monitoring systems intended to safeguard children will only be examined where there is reasonable cause to believe a child is at risk.

Each system will have proportionate access controls and a nominated Information Asset Owner (IAO) who will be responsible for the governance and security of the system. The IAO may authorise other specified staff members to access data held on the systems routinely or on an ad-hoc basis.

### Ad-hoc Requests and Disclosures

An individual's request for surveillance data held about them will be treated as a subject access request (SAR). See Appendix Two.

Requests for surveillance data from an official agency, such as the police or insurance providers, will be processed as ad hoc disclosure requests. We will confirm the purpose of the request and the lawful basis for accessing the data. We may also require formal documentation in support of the request. If we have any concerns about such requests, we will liaise with our Data Protection Officer (DPO).

All requests for surveillance data will be recorded on a log detailing who made the request, the purpose, whether the information was disclosed or refused, and the authorising staff member.

## Record of Processing and Retention

We have a duty under Article 30 of the UK GDPR to ensure that all our data processing activities are recorded for accountability purposes. We maintain an Information Asset Register to fulfil this requirement. We will ensure that the use of surveillance systems is detailed on this register. Any external providers processing surveillance data on our behalf are included in our data processor register.

Surveillance records will only be held as long as necessary to fulfil the specific purpose and deleted in line with our retention schedule.

## Reviews

Surveillance systems must be reviewed annually to ensure they remain necessary, proportionate and effective. We will update the DPIAs to reflect any changes in system use or data collection type. The relevant IAO is responsible for ensuring reviews are completed, and evidence of this is maintained.

The checklist included in Appendix 5 of this document will be used to review our surveillance camera systems.

# Appendix 5 - Surveillance Camera System Checklist

**School Name:**

| **Name and Description of Surveillance System:** | | |
|---|---|---|
| The system addresses the purpose and requirements (i.e., the cameras record the required information). | **YES** | **NO** |
| | **Notes:** | |
| The system is fit for purpose and produces clear images of adequate resolution. | **YES** | **NO** |
| | **Notes:** | |
| Cameras are sited in effective positions to fulfil their task. | **YES** | **NO** |
| | **Notes:** | |
| Cameras are positioned so that they avoid capturing the images of persons not visiting the premises and/or neighbouring properties. | **YES** | **NO** |
| | **Notes:** | |
| Visible signs show that cameras are in operation. These signs include:<br>● Who operates the system<br>● Their contact details<br>● The purpose of the system. | **YES** | **NO** |
| | **Notes:** | |
| Camera recordings are securely stored and access limited. | **YES** | **NO** |
| | **Notes:** | |
| The system has the capability to fulfil a request for an individual's own | **YES** | **NO** |

| | | |
|---|---|---|
| personal information or an ad-hoc disclosure. | **Notes:** | |
| The system has a set retention period, and records outside of retention are deleted. | **YES** | **NO** |
| | **Notes:** | |
| Authorised users can selectively delete information inside the retention period to fulfil the right to erasure. | **YES** | **NO** |
| | **Notes:** | |
| All operators have been authorised by the Information Asset Owner and have completed their mandatory data protection training. | **YES** | **NO** |
| | **Notes:** | |
| The system has been added to the Trust's / school's IAR and the data processing register | **YES** | **NO** |
| | **Notes:** | |

| | |
|---|---|
| **Checklist completed by:**<br><br>Name:<br>Job Title:<br>Date: | **Checklist reviewed and signed by (Information Asset Owner):**<br><br>Name:<br>Job Title:<br>Date: |

# Appendix 6 - Biometrics

## Introduction

This policy sets out how Pathfinder Multi Academy Trust collects and processes biometric data. The nature of this processing, including what information is processed and for what purpose, is outlined in our privacy notices and Appropriate Policy Document.

We will comply with the additional requirements of sections 26 to 28 of the Protections of Freedoms Act 2012. This includes provisions which relate to the use of biometric data in schools and colleges who use an automated biometric recognition system. These provisions are in addition to data protection legislation.

## Definition of Biometric Data

Biometric data is defined as personal data relating to the physical, physiological or behavioural characteristic of an individual which allows the identification of that individual. This can include their fingerprints, facial shape, retina and iris patterns, and hand measurements.

An automated biometric recognition system uses technology which measures an individual's physical or behavioural characteristics by using equipment that operates 'automatically' (i.e. electronically). Information from the individual is automatically compared with biometric information stored in a system to see if a match exists to recognise or identify the individual. For example, where a fingerprint is used to identify an individual and allow them access to an account.

Biometric data is defined in the UK GDPR and the Data Protection Act 2018 as a special category of personal data, and it therefore requires additional measures to be put in place to process it.

## Definition of Processing

Processing of biometric information includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including, but not limited to, disclosing, deleting, organising, or altering it. An automated biometric recognition system processes data when:

a) Recording pupils' biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner,
b) Storing pupils' biometric information on a database system, or
c) Using that data as part of an electronic process, for example, by comparing it with biometric information stored on a database to identify or recognise pupils.

We process the following biometric data:

- Fingerprints – for making cashless payments, and/or accessing electronic devices (secondary schools only)

Any processing of biometric data will only be carried out where there is a lawful purpose for the processing, as defined in data protection legislation.

## Lawful basis - explicit consent

As per guidance from the Department for Education (Protection of biometric data of children in schools and colleges 2022), where a pupil is below the age of 18, consent for the processing of biometric data will be sought from the pupil's parents or carers. Consent for processing of any other individual's biometric data (such as staff) will be sought directly.

We will ensure that members of staff, or the student and both of their parents or carers (if possible) will be informed of our intention to process the individual's biometric data. This will be carried out through readily available privacy notices and communications, prior to or at the point of obtaining consent, and will include:

- The type of biometric data
- What it will be used for
- The individual's rights to withdraw or refuse consent
- What the alternative arrangement will be if consent is refused or withdrawn

Under no circumstances will we collect or process the biometric data of an individual without their explicit consent or the consent of at least one authorised parent or carer, this will be obtained prior to obtaining any biometric data. If one parent objects in writing, then we will not take or use that child's biometric data.

We will ensure that consent is clear and transparent and can be withdrawn at any time, in accordance with UK GDPR. We will regularly review consents to check that the relationship, the processing, and the purposes have not changed.

If a student under 18 objects to the processing of their biometric data, this will override the consent of the parents or guardians, and processing will not continue under any circumstances.

We will ensure that alternative solutions are presented to staff, pupils, and parents when consent is sought, allowing individuals to provide or refuse consent freely. Any alternative solution that is provided will not disadvantage the individual.

### Data Protection by design and default

We will adopt a data protection by design and default approach to processing biometric data. We will consider data protection and privacy risks from the outset and throughout the processing period.

When a new system involving biometric data or a new form of biometric data processing is introduced, we will ensure that a DPIA is completed before implementing the project. This addresses any associated risks and considers the potential impact the processing may have on pupils, staff, and the wider community.

We will be open and transparent about using biometrics and identify whether we are a controller or joint controller of the information. When we use external providers to process data on our behalf, we will have a written contract that meets the requirements of Article 28 of the UK GDPR. We will only use providers who can ensure they have appropriate measures to safeguard the data.

### Bias and/or discrimination

We understand that there may be bias or discrimination when using systems which utilise biometric data. To mitigate any risk resulting from bias and discrimination, we will:

- Ensure that systems have been trained using a sufficient volume and variety of data, use bias-mitigation techniques, and implement fairness metrics.
- Be open and transparent about any known biases.
- Integrate human oversight to review and validate outputs.

We will only process biometric data where we have deemed it necessary and proportionate. We will also consider whether we need to complete an Equalities Impact Assessment to fulfil our obligations under the Equalities Act 2010.

## Retention and destruction

Biometric data will be encrypted and stored securely to prevent unauthorised or unlawful use. It will only be used for the purpose for which it was obtained. Our security measures will be regularly tested to ensure they remain effective.

Biometric data will be securely destroyed when consent is withdrawn or when processing is no longer required for its intended purpose, for example, when the pupil no longer uses the system or has left the school.

.