GDPR Data Protection Policy

Document Date: 1st January 2024
Version: 1.3

Policy Reviewed and Adopted by Governing Board: 5th February 2024

Date of Next Review: 31st December 2025
Responsible Officer: Business Manager, R Foxton

Introduction

Hawes Side Academy is committed to establishing and implementing arrangements to ensure that the responsibilities under the General Data Protection Regulation (GDPR) and other relevant legislation are met.

The overall aim is to ensure that all reasonable measures are taken, as far as reasonably practicable, to ensure the appropriate processing of data in relation to pupils, staff and visitors of the Academy.

Purpose of this policy

The types of personal data that we may be required to handle include information about pupils, parents, our workforce, and others that we deal with. The personal data which we hold is subject to certain legal safeguards specified in the General Data Protection Regulation ('GDPR'), the Data Protection Act 2018 and other regulations (together 'Data Protection Legislation').

Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities as an academy, we will collect, store and process personal data about our pupils, workforce, parents and others. This makes us a data controller in relation to that personal data. We are committed to the protection of all personal data and special category personal data for which we are the data controller.

The law imposes significant fines for failing to lawfully process and safeguard personal data and failure to comply with this policy may result in those fines being applied.

This policy and any other documents referred to in it set out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.
This policy does not form part of any employee's contract of employment and may be amended at any time.
This policy sets out rules on data protection and the legal conditions that must be satisfied when we process personal data.

Legal framework

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

1. The General Data Protection Regulation (GDPR)
2. Data Protection Act 2018 (DPA)
3. The Freedom of Information Act 2000
4. The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
5. The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
6. The Academy Standards and Framework Act 1998
7. The Privacy and Electronic Communications (EC Directive) Regulations 2003
8. Protection of Freedoms Act 2012
9. DfE (2023) 'Keeping children safe in education 2023'

This policy will also have regard to the following guidance:

1. Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
2. Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'
3. ICO (2022) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
4. ICO (2012) 'IT asset disposal for organisations'
5. DfE (2023) 'Data protection in academies'

Linked Documentation

This policy will be implemented in conjunction with the following other academy policies:

1. Online safety Policy
1. Freedom of Information Policy and publication scheme
2. Records Management Policy

Written with due regard to the Equality Act 2010 and Prevent Duty 2015

3. Acceptable Use Policy
4. CCTV policy
5. Child Protection and Safeguarding Policy
6. Records Management Policy
7. Data security and breach policy

Roles and Responsibilities

It is the responsibility of all members of our workforce must comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary or other action.

Data protection officer (DPO)

As an academy, we are required to appoint a Data Protection Officer ("DPO"). Our DPO is Rebecca Foxton, and they can be contacted at Hawes Side Academy, Johnsville Avenue, Blackpool FY4 3LN.

The individual appointed as DPO will have professional experience and be highly knowledgeable about data protection law, particularly that in relation to academies. An existing employee will be appointed to the role of DPO provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests.

The DPO will operate independently and will not be dismissed or penalised for performing their duties. Sufficient resources and appropriate access will be provided to the DPO to enable them to meet their UK GDPR obligations.

The DPO will report to the highest level of management at the academy, which is the governing board.

Staff will ensure that they involve the DPO in all data protection matters closely and in a timely manner.

The DPO is responsible for ensuring compliance with the Data Protection Legislation and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPO.

The DPO is also the central point of contact for all **data subjects** and others in relation to matters of data protection. The DPO will act as the first point of contact for the ICO and for individuals whose data is being processed.

The DPO is responsible for:

- Coordinating a proactive and preventative approach to data protection.
- Calculating and evaluating the risks associated with the academy's data processing.
- Having regard to the nature, scope, context, and purposes of all data processing.
- Prioritising and focussing on more risky activities, e.g. where special category data is being processed.
- Promoting a culture of privacy awareness throughout the academy community.
- Carrying out ad hoc reviews of data practices to ensure staff understand and are acting in accordance with relevant data protection laws

Definitions

All defined terms in this policy are indicated in bold text, and a list of definitions is included in the Appendix to this policy.

Related Procedures

Key Principles

Anyone **processing personal data** must comply with the data protection principles. These provide that **personal data** must be:

- **Processed** fairly and lawfully and transparently in relation to the **data subject**;
- **Processed** for specified, lawful purposes and in a way which is not incompatible with those purposes;
- Adequate, relevant and not excessive for the purpose;
- Accurate and up to date;
- Not kept for any longer than is necessary for the purpose; and
- **Processed** securely using appropriate technical and organisational measures.

Personal Data must also:

- be **processed** in line with **data subjects'** rights;

- not be transferred to people or organisations situated in other countries without adequate protection.

We will comply with these principles in relation to any **processing** of **personal data** by the Trust.

Fair and lawful processing

Data Protection Legislation is not intended to prevent the **processing** of **personal data**, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

For **personal data** to be **processed** fairly, **data subjects** must be made aware:

- that the **personal data** is being **processed**;
- why the **personal data** is being **processed**;
- what the lawful basis is for that **processing** (see below);
- whether the **personal data** will be shared, and if so with whom;
- the period for which the **personal data** will be held;
- the existence of the **data subject's** rights in relation to the **processing** of that **personal data**; and
- the right of the **data subject** to raise a complaint with the Information Commissioner's Office in relation to any **processing**.

We will only obtain such **personal data** as is necessary and relevant to the purpose for which it was gathered, and will ensure that we have a lawful basis for any **processing**.

For **personal data** to be **processed** lawfully, it must be **processed** on the basis of one of the legal grounds set out in the Data Protection Legislation. We will normally **process personal data** under the following legal grounds:

- The consent of the data subject has been obtained
- where the **processing** is necessary for the performance of a contract between us and the **data subject**, such as an employment contract;
- where the **processing** is necessary to comply with a legal obligation that we are subject to, (e.g. the Education Act 2011);
- where the law otherwise allows us to **process** the **personal data** or we are carrying out a task in the public interest; and
- Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject – this condition is not available to processing undertaken by the academy in the performance of its tasks

When **special category personal data** is being processed then an additional legal ground must apply to that processing. We will normally only **process special category personal dat**a under following legal grounds:

- where the **processing** is necessary for employment law purposes, for example in relation to sickness absence;
- where the **processing** is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment;
- where the **processing** is necessary for health or social care purposes, for example in relation to pupils with medical conditions or disabilities; and
- where none of the above apply then we will seek the consent of the **data subject** to the **processing** of their **special category personal data**.

Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent
- Processing relates to personal data manifestly made public by the data subject
- Processing is necessary for:

- Carrying out obligations under employment, social security or social protection law, or a collective agreement
- Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
- The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
- Reasons of substantial public interest with a basis in law which is proportionate to the aim pursued and which contains appropriate safeguards
- The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services with a basis in law
- Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
- Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with a basis in law

- When none of the above apply, consent will be obtained by the data subject to the processing of their special category personal data.

We will inform **data subjects** of the above matters by way of appropriate privacy notices which shall be provided to them when we collect the data or as soon as possible thereafter, unless we have already provided this information such as at the time when a pupil joins us.
If any **data user** is in doubt as to whether they can use any personal data for any purpose then they must contact the DPO before doing so.

The academy will only process personal data without consent where any of the above purposes cannot reasonably be achieved by other, less intrusive means or by processing less data.

Vital Interests

There may be circumstances where it is considered necessary to **process personal data** or **special category personal data** in order to protect the vital interests of a **data subject**. This might include medical emergencies where the **data subject** is not in a position to give consent to the **processing**. We believe that this will only occur in very specific and limited circumstances. In such circumstances we would usually seek to consult with the DPO in advance, although there may be emergency situations where this does not occur.

Consent

Where none of the other bases for **processing** set out above apply then the academy must seek the consent of the **data subject** before **processing** any **personal data** for any purpose.
There are strict legal requirements in relation to the form of consent that must be obtained from **data subjects**.
Consent must be a positive indication expressly confirmed in words. It cannot be inferred from silence, inactivity, a positive action without words or pre-ticked boxes. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes. Consent can be withdrawn by the individual at any time.
Where consent is given, a record will be kept documenting how and when consent was given, and what the data subject was told.
The academy ensures that consent mechanisms meet the standards of the UK GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease. Consent accepted under the DPA will be reviewed to ensure it meets the standards of the UK GDPR; however, acceptable consent obtained under the DPA will not be reobtained.
When pupils and or staff join the Trust, a consent form will be required to be completed in relation to them. This consent form deals with the taking and use of photographs and videos of them, amongst other things. Where appropriate third parties may also be required to complete a consent form.

In relation to all pupils under the age of 12 years old we will seek consent from an individual with parental responsibility for that pupil.

We will generally seek consent directly from a pupil who has reached the age of 12, however we recognise that this may not be appropriate in certain circumstances and therefore may be required to seek consent from and individual with parental responsibility.
If consent is required for any other **processing** of **personal data** of any **data subject** then the form of this consent must:

- Inform the **data subject** of exactly what we intend to do with their **personal data**;
- Require them to positively confirm that they consent – we cannot ask them to opt-out rather than opt-in; and
- Inform the **data subject** of how they can withdraw their consent.

Any consent must be freely given, which means that we cannot make the provision of any goods or services or other matter conditional on a **data subject** giving their consent.
The DPO must always be consulted in relation to any consent form before consent is obtained.
A record must always be kept of any consent, including how it was obtained and when.

Processing for limited purposes

In the course of our activities as a Trust, we may collect and process the personal data set out in our Schedule of Processing Activities. This may include personal data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and personal data we receive from other sources (including, for example, local authorities, other academies, parents, other pupils or members of our workforce).
We will only process personal data for the specific purposes set out in our Schedule of Processing Activities or for any other purposes specifically permitted by Data Protection Legislation or for which specific consent has been provided by the data subject.

Notifying data subjects

If we collect **personal data** directly from **data subjects**, we will inform them about:

- our identity and contact details as **Data Controller** and those of the DPO;
- the purpose or purposes and legal basis for which we intend to **process** that **personal data**;
- the types of third parties, if any, with which we will share or to which we will disclose that **personal data**;
- whether the **personal data** will be transferred outside the European Economic Area ('**EEA**') and if so the safeguards in place;
- the period for which their **personal data** will be stored, by reference to our Retention and Destruction Policy;
- the existence of any automated decision making in the **processing** of the **personal data** along with the significance and envisaged consequences of the **processing** and the right to object to such decision making; and
- the rights of the **data subject** to object to or limit processing, request information, request deletion of information or lodge a complaint with the ICO.

Unless we have already informed data subjects that we will be obtaining information about them from third parties (for example in our privacy notices), then if we receive personal data about a data subject from other sources, we will provide the data subject with the above information as soon as possible thereafter, informing them of where the personal data was obtained from.

Adequate, relevant and non-excessive processing

We will only collect **personal data** to the extent that it is required for the specific purpose notified to the **data subject**, unless otherwise permitted by Data Protection Legislation.

Accurate data

We will ensure that **personal data** we hold is accurate and kept up to date.
We will take reasonable steps to destroy or amend inaccurate or out-of-date data.
Data subjects have a right to have any inaccurate **personal data** rectified. See further below in relation to the exercise of this right.

Timely processing

We will not keep **personal data** longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all **personal data** which is no longer required.

We shall seek to comply with the rights exercised by data subjects as set out below as soon as possible and within legal time limits. However, there may be instances where due to circumstances outside of the Trust's control this may not be possible e.g. where the Academy or Trust has been closed or is only partially operable. In such circumstances data subjects till be notified and provided details about the reason for the delay and when a response can reasonably be expected.

Processing in line with data subjects' rights

We will **process** all **personal data** in line with **data subjects'** rights, in particular their right to:

- request access to any **personal data** we hold about them;
- object to the **processing** of their **personal data**, including the right to object to direct marketing;
- have inaccurate or incomplete **personal data** about them rectified;
- restrict **processing** of their **personal data**;
- have **personal data** we hold about them erased
- have their **personal data** transferred; and
- object to the making of decisions about them by automated means.

The right to be informed

Adults and children have the same right to be informed about how the academy uses their data. The privacy notices supplied to individuals, including children, in regard to the processing of their personal data will be written in clear, plain, age-appropriate language which is concise, transparent, easily accessible and free of charge.

In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller, the controller's representative, where applicable, and the DPO
- The purpose of, and the lawful basis for, processing the data
- The legitimate interests of the controller or third party
- Any recipient or categories of recipients of the personal data
- Details of transfers to third countries and the safeguards in place
- The retention period of criteria used to determine the retention period
- The existence of the data subject's rights, including the right to:
  - Withdraw consent at any time
  - Lodge a complaint with a supervisory authority
- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences

Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided – this information will be supplied at the time the data is obtained.

Where data is not obtained directly from the data subject, information regarding the categories of personal data that the academy holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided – this information will be supplied:

- Within one month of having obtained the data.
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
- If the data are used to communicate with the individual, at the latest, when the first communication takes place.

The right of access

Individuals, including children, have the right to obtain a copy of their personal data as well as other supplementary information, including confirmation that their data is being processed, and the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing. The academy will verify the identity of the person making the request before any information is supplied.

A copy of the information will be supplied to the individual free of charge; however, the academy may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual requests further copies of the same information. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged. All fees will be based on the administrative cost of providing the information.
Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.
Where a SAR has been made for information held about a child, the academy will evaluate whether the child is capable of fully understanding their rights. If the academy determines the child can understand their rights, it will respond directly to the child.
All requests will be responded to without delay and at the latest, within one month of receipt. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.
Where a request is manifestly unfounded or excessive, the academy holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

The academy will ensure that information released in response to a SAR does not disclose personal data of another individual. If responding to the SAR in the usual way would disclose such data, the academy will:

- Omit certain elements from the response if another individual's personal data would be disclosed otherwise.
- Reject requests that cannot be fulfilled without disclosing another individual's personal data, unless that individual consents or it is reasonable to comply without consent.
- Explain to the individual who made the SAR why their request could not be responded to in full.

In the event that a large quantity of information is being processed about an individual, the academy will ask the individual to specify the information the request is in relation to – the time limit for responding to the request will be paused until clarification from the individual is received.

The right to rectification
Individuals, including children, are entitled to have any inaccurate or incomplete personal data rectified.
Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.
Requests for rectification will be investigated and resolved, where appropriate, free of charge; however, the academy may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual makes multiple requests at once. The academy reserves the right to refuse to process requests for rectification if they are manifestly unfounded or excessive or if exemptions apply.

The academy will take reasonable steps to ensure that data is accurate or is rectified if inaccurate, implementing a proportional response for data that has a significant impact on the individual, e.g. if significant decisions are made using that data. The academy will restrict processing of the data in question whilst its accuracy is being verified, where possible. Where the personal data in question has been disclosed to third parties, the academy will inform them of the rectification where possible. Where appropriate, the academy will inform the individual about the third parties that the data has been disclosed to.

Where no action is being taken in response to a request for rectification, or where the request has been investigated and the data has been found to be accurate, the academy will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

The right to erasure
Individuals, including children, hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing. Individuals, including children, have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected or processed

- When the individual withdraws their consent where consent was the lawful basis on which the processing of the data relied
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

The academy will comply with the request for erasure without undue delay and at the latest within one month of receipt of the request.

The academy has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The establishment, exercise or defence of legal claims

The academy has the right to refuse a request for erasure for special category data where processing is necessary for:

- Public health purposes in the public interest, e.g. protecting against serious cross-border threats to health.
- Purposes of preventative or occupational medicine, the working capacity of an employee, medical diagnosis, the provision of health or social care, or the management of health or social care systems or services.

Requests for erasure will be handled free of charge; however, the academy may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual makes multiple requests at once.

As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so. Where personal data has been made public within an online environment, the academy will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

The right to restrict processing

Individuals, including children, have the right to block or suppress the academy's processing of personal data.
The academy will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the academy has verified the accuracy of the data
- Where an individual has objected to the processing and the academy is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restriction instead
- Where the academy no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

If processing is restricted, the academy will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future. The academy will inform individuals when a restriction on processing has been lifted.

Where the academy is restricting the processing of personal data in response to a request, it will make that data inaccessible to others, where possible, e.g. by temporarily moving the data to another processing system or unpublishing published data from a website.

If the personal data in question has been disclosed to third parties, the academy will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.
The academy reserves the right to refuse requests for restricting processing if they are manifestly unfounded or excessive or if exemptions apply. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

The right to data portability
Individuals, including children, have the right to obtain and reuse their personal data for their own purposes across different services. The right to data portability only applies in the following cases:

- Where personal data has been provided directly by an individual to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

Personal data can be easily moved, copied or transferred from one ICT environment to another in a safe and secure manner, without hindrance to usability. Personal data will be provided in a structured, commonly used and machine-readable form. Where feasible, data will be transmitted directly to another organisation at the request of the individual. The academy will not be required to adopt or maintain processing systems which are technically compatible with other organisations.

The academy will provide the information free of charge.
In the event that the personal data concerns more than one individual, the academy will consider whether providing the information would prejudice the rights of any other individual.

The academy will respond to any requests for portability within one month. Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.
Where no action is being taken in response to a request, the academy will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

The right to object
The academy will inform individuals, including children, of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information. Individuals, including children, have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Processing used for direct marketing purposes
- Processing for purposes of scientific or historical research and statistics.

Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.
- The academy will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the academy can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.
- The academy will respond to objections proportionally, granting more weight to an individual's objection if the processing of their data is causing them substantial damage or distress.
- Where personal data is processed for direct marketing purposes:
- The right to object is absolute and the academy will stop processing personal data for direct marketing purposes as soon as an objection is received.

- The academy cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.
- The academy will retain only enough information about the individual to ensure that the individual's preference not to receive direct marketing is respected in future.
- Where personal data is processed for research purposes:
- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the academy is not required to comply with an objection to the processing of the data.

Where the processing activity is outlined above, but is carried out online, the academy will offer a method for individuals to object online.

The DPO will ensure that details are recorded for all objections received, including those made by telephone or in person, and will clarify each objection with the individual making the request to avoid later disputes or misunderstandings. The academy will respond to all objections without undue delay and within one month of receiving the objection; this may be extended by a further two months if the request is complex or repetitive.
Where no action is being taken in response to an objection, the academy will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy

Data security

We will take appropriate security measures against unlawful or unauthorised processing of **personal data**, and against the accidental loss of, or damage to, **personal data**.
We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.
Security procedures include:

- **Entry controls**. Any stranger seen in entry-controlled areas should be reported to the academy office
- **Secure lockable desks and cupboards**. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
- **Methods of disposal**. Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required. IT assets must be disposed of in accordance with the Information Commissioner's Office guidance on the disposal of IT assets.
- **Equipment**. Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.
- **Working away from the academy premises – paper documents.** Staff are expected to limit the taking paper records including personal data off the academy premises to a minimum. Data taken of site should be logged in the reception prior to leaving the academy.
- **Working away from the academy premises – electronic working**. Laptops are provided to staff who need to work from home. These are password protected and access to the academy network is undertaken via a secure portal.
- **Document printing** - Documents containing **personal data** must be collected immediately from printers and not left on photocopiers.
- **Password protection and security measures**

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

Data protection by design and default

The academy will act in accordance with the UK GDPR by adopting a data protection by design and default approach and implementing technical and organisational measures which demonstrate how the academy has considered and integrated data protection into all aspects of processing activities. In line with the data protection by default approach, the academy will ensure that only data that is necessary to achieve its specific purpose will be processed.
The academy will implement a data protection by design and default approach by using a number of methods, including, but not limited to:

- Considering data protection issues as part of the design and implementation of systems, services and practices.
- Making data protection an essential component of the core functionality of processing systems and services.
- Automatically protecting personal data in academy ICT systems.
- Implementing basic technical measures within the academy network and ICT systems to ensure data is kept secure.
- Promoting the identity of the DPO as a point of contact.
- Ensuring that documents are written in plain language so individuals can easily understand what is being done with personal data.

Data Protection Impact Assessments

The Trust takes data protection very seriously, and will consider and comply with the requirements of Data Protection Legislation in relation to all of its activities whenever these involve the use of personal data, in accordance with the principles of data protection by design and default.
In certain circumstances the law requires us to carry out detailed assessments of proposed **processing**. This includes where we intend to use new technologies which might pose a high risk to the rights of **data subjects** because of the types of data we will be **processing** or the way that we intend to do so.
The Trust will complete an assessment of any such proposed **processing** and has a template document which ensures that all relevant matters are considered.

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

DPIAs will allow the academy to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the academy reputation which might otherwise occur. A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals, and will be used for more than one project, where necessary.
High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences
- The use of CCTV

The academy will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

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

Data breaches

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The principal will ensure that all staff are made aware of, and understand, what constitutes a data breach as part of their training.
Effective and robust breach detection, investigation and internal reporting procedures are in place at the academy, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.
Where the academy faces a data security incident, the DPO will coordinate an effort to establish whether a personal data breach has occurred, assess the significance of any breach, and take prompt and appropriate steps to address it.
All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the academy becoming aware of it. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed, and the individuals concerned will be contacted directly. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority. The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be

assessed on a case-by-case basis. In the event that a breach is sufficiently serious, the public will be notified without undue delay.
Within a breach notification to the supervisory authority, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

Where notifying an individual about a breach to their personal data, the academy will provide specific and clear advice to individuals on the steps they can take to protect themselves and their data, where possible and appropriate to do so.
The academy will ensure all facts regarding the breach, the effects of the breach and any decision-making processes and actions taken are documented in line with the UK GDPR accountability principle and in accordance with the Records Management Policy.
Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.
The academy will work to identify the cause of the breach and assess how a recurrence can be prevented, e.g. by mandating data protection refresher training where the breach was a result of human error.

Disclosure and sharing of personal information

We may share **personal data** that we hold about **data subjects**, and without their consent, with other organisations. Such organisations include the Department for Education, Education and Skills Funding Agency "ESFA", Ofsted, health authorities and professionals, the Local Authority, examination bodies, other academies, and other organisations where we have a lawful basis for doing so.
The Trust will inform **data subjects** of any sharing of their **personal data** unless we are not legally required to do so, for example where **personal data** is shared with the police in the investigation of a criminal offence.
In some circumstances we will not share safeguarding information. Please refer to our Child Protection Policy.
Further detail is provided in our Schedule of Processing Activities.

Publication of information

The academy publishes a Freedom of Information Publication Scheme on its website outlining classes of information that will be made routinely available, including:
Policies and procedures.
Minutes of meetings.
Annual reports.
Financial information.
Classes of information specified in the Freedom of Information Publication Scheme are made available quickly and easily on request.
The academy will not publish any personal information, including photos, on its website without the permission of the affected individual. When uploading information to the academy website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

Data Processors

We contract with various organisations who provide services to the Trust (see appendix 2).
In order that these services can be provided effectively we are required to transfer **personal data** of **data subjects** to these **data processors**.
Personal data will only be transferred to a **data processor** if they agree to comply with our procedures and policies in relation to data security, or if they put in place adequate measures themselves to the satisfaction of the Trust. The Trust will always undertake due diligence of any **data processor** before transferring the **personal data** of **data subjects** to them. Contracts with **data processors** will comply with Data Protection Legislation and contain explicit obligations on the **data processor** to ensure compliance with the Data Protection Legislation, and compliance with the rights of **Data Subjects**.

Automated decision making and profiling

The academy will only ever conduct solely automated decision making with legal or similarly significant effects is the decision is:

- Necessary for entering into or performance of a contract.
- Authorised by law.
- Based on the individual's explicit consent.

Automated decisions will not concern a child nor use special category personal data, unless:

- The academy has the explicit consent of the individual.
- The processing is necessary for reasons of substantial public interest.

The academy will conduct a DPIA for automated decision making to mitigate risk of errors, bias and discrimination.
The academy will ensure that individuals concerned are given specific information about the processing and an opportunity to challenge or request a review of the decision.
Individuals have the right not to be subject to a decision when both of the following conditions are met:

- It is based on automated processing, e.g. profiling
- It produces a legal effect or a similarly significant effect on the individual

The academy will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.
When automatically processing personal data for profiling purposes, the academy will ensure that the appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.
- Using appropriate mathematical or statistical procedures.
- Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

CCTV and photography

The academy understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.
The academy notifies all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email. Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.
All CCTV footage will be kept for six months for security purposes; the SBM is responsible for keeping the records secure and allowing access.
Before the academy is able to obtain the data of pupils or staff, it is required to give notification and obtain consent for this Special Category Data due to additional requirements for processing such data under the Protection of Freedoms Act 2012.
The academy will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them. If the academy wishes to use images or video footage of pupils in a publication, such as the academy website, prospectus, or recordings of academy plays, written permission will be sought for the particular usage from the parent of the pupil. Precautions, as outlined in the Photography and Images Policy, are taken when publishing photographs of pupils, in print, video or on the academy website.
Images captured by individuals for recreational or personal purposes, and videos made by parents for family use, are exempt from the UK GDPR.
Parents and others attending academy events are able to take photographs and videos of those events as long as they are for domestic purposes only. Photographs or videos being used for any other purpose are prohibited to be taken by parents or visitors to the academy.
The academy asks that parents and others do not post any images or videos which include any children other than their own on any social media, or otherwise publish those images or videos.

Cloud computing

For the purposes of this policy, 'cloud computing' refers to storing and accessing data and programs, such as documents, photos or videos, over the internet, rather than on a device's hard drive. Cloud computing involves the academy accessing a shared pool of ICT services remotely via a private network or the internet.
All staff will be made aware of data protection requirements and how these are impacted by the storing of data in the cloud, including that cloud usage does not prevent data subjects from exercising their data protection rights.
If the cloud service offers an authentication process, each user will have their own account. A system will be implemented to allow user accounts to be created, updated, suspended and deleted, and for credentials to be reset if they are forgotten, lost or stolen. Access for employees will be removed when they leave the academy.
All files and personal data will be encrypted before they leave a academy device and are placed in the cloud, including when the data is 'in transit' between the device and cloud. A robust encryption key management arrangement will be put in place to maintain protection of the encrypted data. The loss of an encryption key will be reported to the DPO immediately; failure to do so could result in accidental access or destruction of personal data and, therefore, a breach of the relevant data protection legislation.
As with files on academy devices, only authorised parties will be able to access files on the cloud. An audit process will be put in place to alert the academy should unauthorised access, deletion or modification occur, and ensure ongoing compliance with the academy's policies for the use of cloud computing.
The academy's usage of cloud computing, including the service's security and efficiency, will be assessed and monitored by the DPO. The DPO will also ensure that a contract and data processing agreement are in place with the service provider, confirming compliance with the principles of the UK GDPR and DPA. The agreement will specify the circumstances in which the service provider may access the personal data it processes, such as the provision of support services.
The DPO will also:

- Ensure that the service provider has completed a comprehensive and effective self-certification checklist covering data protection in the cloud.
- Ensure that the service provider can delete all copies of personal data within a timescale in line with the academy's Data Protection Policy.
- Confirm that the service provider will remove all copies of data, including back-ups, if requested.
- Find out what will happen to personal data should the academy decide to withdraw from the cloud service in the future.
- Assess the level of risk regarding network connectivity and make an informed decision as to whether the academy is prepared to accept that risk.
- Monitor the use of the academy's cloud service, with any suspicious or inappropriate behaviour of pupils, staff or parents being reported directly to the principal

Data retention

Data will be managed in line with the academy Records Management Policy.

Data will not be kept for longer than is necessary.

Unrequired data will be deleted as soon as practicable.

Some educational records relating to former pupils or employees of the academy may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

Disclosure and Barring Service (DBS) data

All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

Data provided by the DBS will never be duplicated.

Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

Safeguarding

The academy understands that the UK GDPR does not prevent or limit the sharing of information for the purposes of keeping children safe.

The academy will ensure that staff have due regard to their ability to share personal information for safeguarding purposes, and that fears about sharing information must not be allowed to obstruct the need to safeguard and protect pupils. The governing board will ensure that staff are:

- Confident of the processing conditions which allow them to store and share information for safeguarding purposes, including information, which is sensitive and personal, and should be treated as 'special category personal data'.
- Aware that information can be shared without consent where there is good reason to do so, and the sharing of information will enhance the safeguarding of a pupil in a timely manner.

The academy will ensure that information pertinent to identify, assess and respond to risks or concerns about the safety of a child is shared with the relevant individuals or agencies proactively and as soon as is reasonably possible. Where there is doubt over whether safeguarding information is to be shared, especially with other agencies, the DSL will ensure that they record the following information:

- Whether data was shared
- What data was shared
- With whom data was shared
- For what reason data was shared
- Where a decision has been made not to seek consent from the data subject or their parent
- The reason that consent has not been sought, where appropriate

The academy will aim to gain consent to share information where appropriate; however, staff will not endeavour to gain consent if to do so would place a child at risk. The academy will manage all instances of data sharing for the purposes of keeping a child safe in line with the Child Protection and Safeguarding Policy.

Pupils' personal data will not be provided where the serious harm test is met. Where there is doubt, the academy will seek independent legal advice

Monitoring and Review

The primary purpose of this policy is to ensure processing of certain information about its staff members and pupils is done so in accordance with the legal obligations of the academy under the General Data Protection Regulation (GDPR).

Monitoring of systems in place will be undertaken through internal quality assurance processes by the Data protection Officer (DPO) and senior team including observation, testing and analysis and review of available data and information. A formal audit will be undertaken at least annually by the Governing body and/or an external team to support the academy and provide feedback to ensure that effective organisation and arrangements are in place.

This policy is reviewed every two years by the DPO, SBM and the Principal.

Appendix 1

DEFINITIONS

Term	Definition
Biometric Data	is information about a person's physical or behavioural characteristics or features that can be used to identify them and is obtained or recorded for the purposes of a biometric recognition system and can include fingerprints, hand shapes, features of the eye or information about a person's voice or handwriting
Biometric Recognition System	is a system that operates automatically (electronically) and:

	• Obtains or records information about a person's physical or behavioural characteristics or features; and • Compares or otherwise processes that information with stored information in order to establish or verify the identity of the person or otherwise determine whether they are recognised by the system
Criminal Data	In the case of criminal offence data, academies are only able to process this if it is either: • Under the control of official authority; or • Authorised by domestic law. The latter point can only be used if the conditions of the reason for storing and requiring the data fall into one of the conditions below: • The processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller of the data subject in connection with employment, social security, social protection, health or social care purposes, public health, and research
Data	is information which is stored electronically, on a computer, or in certain paper-based filing systems
Data Subjects	for the purpose of this policy include all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information
Personal Data	means any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
Data Controllers	are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes
Data Users	are those of our workforce (including Governors and volunteers) whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times
Data Processors	include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions
Processing	is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties
Special Category Personal Data	includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or Biometric Data 'Sensitive personal data' does not include data about criminal allegations, proceedings or convictions
Workforce	Includes, any individual employed by Trust such as staff and those who volunteer in any capacity including Trustees / Members/ Governors/ parent helpers

Appendix 2

CONTRACTS

Management Support/ HR Support

Arbor = Academy MIS
Blackpool Council Annual Services
Blackpool FC Community Trust
Blackpool Teaching Hospitals
Comptech

Communicate
CPOMS
Disclosure Services
DFE
Lancashire County Council: Pension Services
Marsh Insurance
Moore and Smalley Accountants
ParentPay/Cypad = Academy payment system
Paul Duckworth Advisory Service
Questionpro
RPA Insurance
Schools Advisory Service (HR)
Schools Advisory Service (Wellbeing policy)
Shard
Shred It bins= data destruction
Sign in App = sign in system
Strictly Education
STAR Institute
Teachers Pension Service
Up Beat
Vimeo= video sharing tool

Curriculum Software

Create development
Ed Shed
FFT Aspire
IDL
TT Rock Stars
Star Reader
Star Maths
Spelling Shed
Tapestry