ARCHWAY ACADEMY INDEPENDENT SCHOOL
DATA PROTECTION POLICY

Introduction

Archway Academy takes Data Protection and our obligations with regard to Data Protection very seriously.

The school is a Data Controller for the purposes of the UK Data Protection Bill which came into force in May 2018 (Data Protection Act 2018) and the General Data Protection Regulation (GDPR) (together "Data Protection Law") and is registered with the Information Commissioner's Office ("ICO").

The school's Head of Administration (Sharon Saunders) acts as the school's Data Protection Officer and is available to contact on any Data Protection issue by emailing: enquiries@archwayacademy.org.uk or by
calling: 0121 772 7772.

Purpose

This Data Protection Policy regulates and details the way in which Archway Academy obtains, uses, holds, transfers and processes Personal Data and Special Category or Sensitive Personal Data about individuals and ensures that all the school's employees know the rules for protecting Personal Data.

This Policy also describes individuals' rights in relation to their Personal Data processed by the school.

Definitions

"**Personal Data**" is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, online identifier. It can also include pseudonymised data.

"**Special categories of Personal Data**" is data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes).

"**Criminal offence Data**" is data which relates to an individual's criminal convictions and offences.

"**Data processing**" is any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, 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.

Legislation

The school has practices in place in relation to their handling of Personal Data to ensure that they are acting in accordance with UK laws and other relevant regulatory guidance. The most notable legislation in this area is the General Data Protection Regulation (GDPR) and the UK Data Protection Bill (together "Data Protection Law").

The school also maintains an up to date section on Data Protection on the school's website, with copies of its Privacy Notices to different sections of the school community.

The school will comply with the principles of the Data Protection Law to ensure that all data is: - Fairly and lawfully processed - Processed only for lawful purposes - Adequate, relevant and not excessive - Accurate and up to date - Not kept for longer than is necessary - Processed in accordance with the data subject's rights - Secure - Not transferred to other countries without consent and adequate protection.

The school will also comply with these further rights for individuals: - The right to be informed - The right of access - The right to rectification - The right to erasure - The right to restrict processing - The right to data portability - The right to object - Rights in relation to automated decision making and profiling.

At all times, the school will endeavour to ensure that it has a legal basis for the processing of personal information.

Data Protection Principles

Under GDPR, all Personal Data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:

- processing will be fair, lawful and transparent;

- data will be collected for specific, explicit, and legitimate purposes;
- data collected will be adequate, relevant and limited to what is necessary for the purposes of processing;
- data will be kept accurate and up to date. Data which is found to be inaccurate will be rectified or erased without delay;
- data is not kept for longer than is necessary for its given purpose;
- data will be processed in a manner that ensures appropriate security of Personal Data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures.

Personal Data

Personal Data is data relating to a living individual who can be identified from that information or from that data and other information in the school's possession (for example: name, address, telephone number, employee number). It can also include expressions of opinions about an individual. Sensitive or special category Personal Data relates to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, criminal convictions. Personal Data concerning disability is sensitive data.

In order to carry out its routine, ordinary duties to employees, pupils and parents/guardians/carers, the school needs to process a wide range of Personal Data about individuals (including current, past and prospective employees, pupils or parents/guardians/carers) as part of its daily operations.

Dependent on the nature of the school's relationship with the data subject, there will be different reasons and purposes for the school processing Personal Data, the types of data held, how the data is collected, the legal basis for processing the data, who has access to the data, who the data is shared with, the retention period for that data, and the specific subject rights with regard to that data.

Under GDPR, all Data Controllers, including Archway Academy, must have a Lawful Basis for processing Personal Data. The six bases are: Consent, Contractual, Legal Obligation, Vital Interests, Public Tasks and Legitimate Interests. The ICO states that it is the responsibility of the individual organisation to decide on which bases to process data.

Having undertaken a review of the data we hold and the way in which we process it, Archway Academy believes that all of the data held relating to our school community is processed under three bases, namely Legal Obligation, Contractual and/or Legitimate Interests.

For Data Protection purposes, we consider our community to include: prospective, current and former pupils, prospective, current and former parents/guardians/carers, prospective, current and former employees.

Given the nature of the existing relationship we have with our school community, Archway Academy's interpretation is that we can lawfully process information under the three bases mentioned above.

Personal Data will be treated with the utmost integrity, respect and confidentiality. Personal Data will be stored and used in accordance with Privacy Notices that reflect the new regulation and which are available on the school's website:

- Privacy Notice for Pupils;
- Privacy Notice for Parents/Guardians/Carers;
- Privacy Notice for Staff.

Communications will be conducted in the least intrusive way possible and only in ways that would be reasonably expected, as additionally outlined in our Privacy Notices. Where we process children's data, we take extra care to ensure we protect their interests.

We regard the lawful and correct treatment of personal information as very important to our successful operation and to maintaining confidence between us and those with whom we carry out business. We will ensure that we treat personal information lawfully and correctly.

To this end we fully endorse and adhere to the principles of the General Data Protection Regulation (GDPR).

Special Category Personal Data

"Special Category Personal Data" (sometimes called "Sensitive Personal Data") is Personal Data about a person's race or ethnicity, their health, their sexual preference, the medical information, their religious beliefs, their political views, trade union membership or information accusing an individual of any crime, or about any criminal prosecution against them, and the decision of the court and any punishment. The Data Protection Officer can provide further information on what it is, and the handling of, Special Category Personal Data.

Special Category Personal Data should not be collected or used unless essential. It must be treated as strictly confidential. Extra care must be taken with it and it must be kept more securely. In addition to the normal requirements for lawful use of any Personal Data such details should not be used without the explicit prior consent of the individual, which has to be clear, unambiguous and voluntary.

The school does not seek to obtain Special Category Personal Data unless: a) the individual concerned agrees in writing that we may do so, on the basis of a full understanding of why the school is collecting the data b) the school needs to do so to meet its obligations or exercise its rights under any relevant laws; or c) in circumstances such as where the processing is necessary to either safeguard or protect the vital interests of the individual concerned.

Special Category Personal Data should not be disclosed unless measures are taken to encrypt or otherwise secure that information due to the potential for harm or distress if the email is received by unintended recipients or otherwise goes astray.

Special Category Personal Data should be collected and used as little as possible and be subject to more limited and strictly need to know access and used subject to greater security measures than other Personal Data.

Other Personal Data where misuse may lead to distress or harm, especially to fraud or identity theft (for example, bank account or credit card details, or official government identification numbers, such as National Insurance contribution numbers) must be treated like Special Category Personal Data.

Processing of Personal Data

The school uses or processes Personal Data (including Sensitive Personal Data) on a range of individuals for a multitude of business purposes, including the use of CCTV systems. Such individuals may include prospective, current and former: employees and contractors, pupils and parents/guardians/carers, business contacts, customers and prospects, job applicants. The person whose Personal Data is used by the school is known as “the data subject”.

When the school collects, stores, uses, discloses, updates or deletes or destroys Personal Data, this is called ”processing”. All processing is regulated by Data Protection legislation and must meet certain conditions to be carried out lawfully.

Lawful Basis of Processing

We acknowledge that processing may be only be carried out where a lawful basis for that processing exists and we have assigned a lawful basis against each processing activity.

Where no other lawful basis applies, we may seek to rely on the individual’s consent in order to process data.

However, we recognise the high standard attached to its use. We understand that consent must be freely given, specific, informed and unambiguous. Where consent is to be sought, we will do so on a specific and individual basis where appropriate.

Individuals will be given clear instructions on the desired processing activity, informed of the consequences of their consent and of their clear right to withdraw consent at any time.

Personal Data and Transparency

Archway Academy is entrusted to use the Personal Data of individuals on the basis that the proposed use is transparent, expected and clearly defined. Accordingly, one of the main data protection obligations requires the school to process Personal Data fairly.

In addition, use of Personal Data must be lawful. In practice, this means that the school will comply with at least one of the following conditions when processing Personal Data: a) the individual to whom the Personal Data relates has consented to the processing; b) the processing is necessary for the performance of a contract

between the school and the individual (or to enter into that contract at the individual's request); c) the processing is necessary to comply with a legal obligation (not a

contractual obligation) placed on the school; d) the processing is necessary to protect a vital interest of the individual (where there is an imminent risk to their life or of serious harm to them otherwise); or e) the processing is necessary to pursue the legitimate interest of the school (or a proposed recipient of the Personal Data) but where on balance, this would not involve disproportionate harm to the individual.

Use of Personal Data should meet one or more of these conditions. If there are any concerns about this; it is proposed to use Personal Data for additional purposes; or new reasons for using Personal Data are contemplated, reliance on these conditions must be discussed in the first instance with the Data Protection Officer prior to them being relied upon.

All new Personal Data processing activities and projects involving the use of Personal Data must be approved prior to being started as there are complex exemptions and other lawful reasons for processing which may apply. For example, if someone provides their details as a contact, you will not be able to start sending them marketing e - mails unless it is covered in an appropriate notice and consent from that individual.

In addition, the school ensures its Personal Data is accurate and up to date. The school takes care to record and input Personal Data accurately. Some Personal Data may change from time to time (such as addresses and contact details, bank accounts and the place of employment). It is important to keep current records up to date. Archway Academy takes care to update records promptly and correctly.

Records of Processing

The school keeps records of its processing activities. These records will be kept up to date so that they reflect current processing activities.

Privacy ('Fair Processing') Notices

When an individual gives the school any Personal Data about him or herself, the school will make sure the individual knows: a) who is responsible for the Processing of their Personal Data; b) for what purposes that school will process the Personal Data provided to it; c) sufficient details about any proposed disclosures/transfers of their Personal Data to Third Parties; d) the rights that the individual has in respect of their Personal Data; e) any other information that the individual should receive to ensure the processing carried out is within his/her reasonable expectations (retention

periods for instance); and f) who to contact to discuss or raise any Personal Data issue.

The school does this by providing this information is known as providing a “Privacy Notice” or fair processing notice. Before collecting Personal Data, staff at the school will give individuals providing those details appropriate Privacy Notices, these may be embedded in contracts, or on websites or form part of application or other forms. The school will inform individuals about the processing of their Personal Data before or at the time the data is collected. The information contained in its Privacy Notices will be concise and easily accessible and written in clear and plain language.

We will only process Personal Data in a manner and for purposes consistent with the relevant Privacy Notice(s) already provided. Personal Data should not be collected for one purpose and then used for a second purpose unless that is also set out in the relevant notice.

For ease of reference and understanding, the school has produced different Privacy Notices for the different categories of individuals it deals with: pupils, employees, parents/guardians/carers. These can be accessed using the school’s website.

Rights and Contact Details

All data subjects have certain rights under Data Protection Law, including a right to be given access to data held about them by a Data Controller. Other rights will be dependent on the nature of the information given and are more fully explained in the school’s Privacy Notices.

If you have any concerns about the school’s handling of your Personal Data, please contact the school’s Data Protection Officer, Sharon Saunders at:
enquiries@archwayacademy.org.uk
You can also find details of your rights under Data Protection Law at:
www.ico.org.uk

Types of Data held - Employees

We keep several categories of Personal Data on our employees in order to carry out effective and efficient processes. We keep this data in a personnel file relating to each employee and we also hold the data within our computer systems, for example, our BACS salary payment system.

Specifically, we hold the following types of data:

- personal details such as name, address, phone numbers;

- information gathered via the recruitment process such as that entered into a CV or included in a CV cover letter, references from former employers, education details and employment history etc.;

- details relating to pay administration such as National Insurance numbers, bank account details and tax codes;

- medical and/or health information;

- information relating to the employee's employment with us, including:

    - job title and job descriptions;

    - salary;

    - wider terms and conditions of employment;

    - details of formal and informal proceedings, such as letters of concern, disciplinary and grievance proceedings, annual leave records, appraisal and performance information;

    - internal and external training courses and qualifications undertaken.

All of the above information is required for our processing activities. Information on those processing activities is included in the Privacy Notice for employees.

Employee Rights

Employees have the following rights in relation to the Personal Data held on them by the school:

- the right to be informed about the data we hold on them and what we do with it;

- the right of access to the data we hold on them;

- the right for any inaccuracies in the data we hold on them, however they come to light, to be corrected. This is also known as 'rectification';

- the right to have data deleted in certain circumstances. This is also known as ‘erasure’;
- the right to restrict the processing of the data;
- the right to transfer the data we hold on them to another party. This is also known as ‘portability’;
- the right to object to the inclusion of any information;
- the right to regulate any automated decision making and profiling of Personal Data.

Training

New employees must read and understand the policy on Data Protection as part of their induction.

All employees receive training covering basic information about confidentiality, Data Protection and the actions to take upon identifying a potential data breach. (see exemplar - Appendix 1)

The nominated Data Controller for the school is trained appropriately in their role under the GDPR.

All employees who need to use the computer system are trained to protect individuals’ private data, to ensure data security, and to understand the consequences to them as individuals and the school of any potential lapses and breaches of the school’s policies and procedures.

Additional Responsibilities

In order to protect the Personal Data of relevant individuals, those within our business who must process data as part of their role have been made aware of our policies on Data Protection.

We have also appointed individuals with responsibility for reviewing and monitoring our Data Protection systems.

Access to Data

As stated above, individuals have a right to access the Personal Data that we hold on them. To exercise this right, a Subject Access Request should be made. We will comply with the request without delay, and within one month unless, in accordance with legislation, we decide that an extension is required. Those who make a request will be kept fully informed of any decision to extend the time limit.

No charge will be made for complying with a request unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the individual making the request. In these circumstances, a reasonable charge will be applied.

Data Security

All our employees are aware that hard copy personal information should be kept in a locked filing cabinet, drawer, or safe.

Employees are aware of their roles and responsibilities when their role involves the processing of data. All employees are instructed to store files or written information of a confidential nature in a secure manner so that are only accessed by people who have a need and a right to access them and to ensure that screen locks are implemented on all PCs, laptops etc. when unattended. No files or written information of a confidential nature are to be left where they can be read by unauthorised people.

Where data is computerised, it should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

Employees must always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them.

Personal Data relating to employees should not be kept or transported on laptops, USB sticks, or similar devices, unless prior authorisation has been received. Where Personal Data is recorded on any such device it should be protected by:

- ensuring that data is recorded on such devices only where absolutely necessary;

- using an encrypted system - a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted;

- ensuring that laptops or USB drives are not left where they can be stolen.

Failure to follow the school's rules on data security may be dealt with via the school's disciplinary procedure. Appropriate sanctions include dismissal (with or without notice) dependent on the severity of the failure.

Data Retention and Archives

Personal Data must be stored securely and not be kept for any longer than required. Some records have to be retained for minimum periods by law (such as records on employee payments and their taxation under tax laws).

As a general rule, when Personal Data is no longer needed for the purposes for which it was collected, this Personal Data will be securely and permanently destroyed as soon as practicable.

The school will not delete or destroy or amend records containing Personal Data without explicit consent once they have been informed those records have been requested by the individual whose Personal Data it is, or by a Data Protection Authority. Such a breach may be a criminal offence with personal liability.

The Right to Information, the Right to Erasure and Subject Access Requests

Individuals have certain rights in relation to their Personal Data:
a) the right to obtain information (what Personal Data, from where, used for what purposes and shared with which recipients) about Personal Data held about themselves and to obtain copies of such Personal Data (Subject Access Request); b) the right to prevent processing of Personal Data for direct marketing purposes; c) the right to object to and stop certain processing of Personal Data where it is likely to cause substantial unwarranted harm or distress; d) the right to have Personal Data corrected; e) the right to compensation for any damage/distress suffered from any breach; f) the right to be informed of automated decision making about them.

If any member of school staff receives such a request or demand from an individual, they must promptly inform the Data Protection Officer.

Individuals are also allowed to withdraw their consent (where this is not required for the school's legitimate interests) to the school's use of their Personal Data at any

time. If a school employee receives such a withdrawal of consent, they must promptly inform the Data Protection Officer.

If anyone at the school receives a request to stop sending marketing materials, direct marketing communications of that type to that individual must be stopped as soon as is possible.

Individuals can also ask in writing for copies of their Personal Data which the school holds about them and other details about how the school uses their Personal Data.

Subject to receipt of proof of ID where considered necessary (and payment of any official fee permitted which the school has requested), following receipt of a written request from an individual for access to his/her Personal Data, the school will (to the extent requested by the individual): (a) inform that individual whether the school holds Personal Data about him or her; (b) describe the Personal Data about the individual which it holds, the reason for holding the Personal Data and the categories of persons to whom it may disclose the Personal Data; and (c) provide the individual with copies of the Personal Data held about him or her, together with an indication of the source(s) of the Personal Data.

Strict rules must be followed as part of this process. Therefore, any such request received should be passed on to the Data Protection Officer. There are strict statutory deadlines for responding. School staff must not respond to any such request directly.

There is a right under Data Protection Law known as “the right to be forgotten”. This gives an individual the right to have their data erased when there is no compelling reason for continued processing.

Third Party Processing

Where we engage third parties to process data on our behalf, we will ensure, via a data processing agreement with the third party, that the third party takes such measures in order to maintain the school’s commitment to protecting data.

International Data Transfers

Archway Academy does not transfer Personal Data to any recipients outside of the EEA.

Requirement to notify breaches

All data breaches will be recorded on our Data Breach Register. Where legally required, we will report a breach to the Information Commissioner within 72 hours of discovery. In addition, where legally required, we will inform the individual whose data was subject to breach.

Appendix 1.

Key Summary and Top Tips for Archway Academy Staff - Data Protection

Key Summary

80% of data breaches involve staff within an organisation (figure from the Information Commissioner's Office) and breaches, for the most part, are unintentional. Therefore, everyone dealing with Personal Data needs to have a basic understanding of the Data Protection Law.

Archway Academy collects a variety of Personal Data on pupils, parents, contractors, staff, volunteers, business contacts etc. for perfectly legitimate business reasons in connection with the running of the school. It is vital that all this information is kept securely, is regularly reviewed and disposed of when no longer required.

Top Data Protection Tips

1. Read and follow the School's Data Protection Policy.
2. Use strong passwords on all devices and two step authentication wherever possible. Ensure that any device you access school Personal Data on (mobiles for instance) are password protected.
3. It is preferable not to, but if you do use portable memory devices, ensure these are encrypted (memory sticks, hard drives etc.; your Line Manager can advise on the procedure for this).
4. Do not download Personal Data onto personally owned devices or send e mails to home e mail addresses unless absolutely necessary. In such cases, any Personal Data should be permanently deleted from the personal device as soon as is possible after use.
5. Only keep information as long as necessary - conduct periodic reviews (at least yearly) of personal systems (paper and electronic) and delete Personal Data that is no longer required.
6. Remember that most data breaches are unintentional - double check who you are sending information to, don't leave computers unattended and unlocked and make sure you shred confidential information when it is no longer required.

7. Before sharing any personal information (this includes photos and/or images), check that the school has the relevant permission to do so.
8. If in any doubt about any Personal Data issue, contact the School's Data Protection Officer.

Further Advice

Tips on keeping information secure

1. Keep passwords secure - change these regularly and do not share or give other people your password. Use two step authentication.
2. Always lock/log off computers when away from your desk.
3. Dispose of confidential paper waste securely by shredding.
4. Prevent virus attacks by taking care when opening emails and attachments or visiting new websites.
5. Hard copy personal information should be stored securely when it is not being used (lockable cabinets etc.).
6. Be careful when discussing individuals that you are not in earshot of anyone who does not need access to that information.
7. Position computer screens away from windows and walkways to prevent accidental disclosures of personal information.
8. Encrypt personal information that is being taken or sent outside the school or office.
9. Do not, unless absolutely necessary, download Personal Data to a non-school device.

Tips on keeping only relevant information

1. Collect only the personal information required.
2. Explain new or changed business purposes to pupils, parents/guardians/carers, employees and others, and obtain consent or provide an opt-out or opt-in where appropriate.
3. Update records promptly - for example, changes of address, phone numbers.
4. Delete personal information the school no longer requires. If in doubt, please check whether the information should be retained.
5. In the case of Safeguarding information, this should always be passed to the Designated Safeguarding Lead (DSL) for them to decide whether or not the information should be retained.


ARCHWAY