ASHBY SCHOOL DATA PROTECTION POLICY

Title of Policy	Data Protection Policy
Last reviewed	Autumn 2020
Originator	Andrew Burton
Date of review	Autumn 2021
Additional information	Refer to privacy notices

ASHBY SCHOOL DATA PROTECTION POLICY INDEX

ASHBY SHOOL DATA PROTECTION POLICY

A. General Statement

1) Ashby School is required to keep and process certain information about its staff members and students in accordance with its legal obligations under the General Data Protection Regulation (GDPR).

2) The Academy may, from time to time, be required to share personal information about its staff or students with other organisations, mainly the LA, other schools and educational bodies, and potentially social services.

3) The Academy has a duty to be registered, as Data Controller, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website. The Academy also has a duty to issue a Fair Processing Notice to all students/parents; this summarises the information held on students, why it is held and the other parties to whom it may be passed on.

4) This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the Academy complies with the following core principles of the GDPR and complies with the new requirements which came into effect on 25 May 2018. The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

B. Definition of Personal Data

1) Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held. For the purpose of this policy, personal data refers to information that relates to an identifiable, living individual, including information such as an online identifier, such as an IP address.

2) The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

3) Sensitive personal data is referred to in the GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data and data concerning health matters.

C. Legal framework

1) This policy has due regard to legislation, including, but not limited to the following:
   - The General Data Protection Regulation (GDPR)
   - The Freedom of Information Act 2000
   - The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
   - The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
   - The School Standards and Framework Act 1998

2) This policy will be implemented in conjunction with the following other Academy policies:
   - E-Safety Policy
   - Freedom of Information Policy
   - Safeguarding Policy

D. Data Protection Principles

1) The Data Protection Act 1998 establishes **'the eight'** enforceable principles that must be adhered to at all times:
   - Personal data shall be processed fairly and lawfully;

- Personal data shall be obtained only for one or more specified and lawful purposes;
- Personal data shall be adequate, relevant and not excessive;
- Personal data shall be accurate and where necessary, kept up to date;
- Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;
- Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998;
- Personal data shall be kept secure i.e. protected by an appropriate degree of security;
- Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

E. Maintaining the Data Protection Principles

1) The Academy is committed to maintaining the above principles at all times. Therefore the Academy will:
   - Inform individuals why the information is being collected when it is collected
   - Inform individuals when their information is shared, and why and with whom it was shared
   - Check the quality and the accuracy of the information it holds
   - Ensure that information is not retained for longer than is necessary
   - Ensure that when obsolete information is destroyed that it is done so appropriately and securely
   - Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
   - Share information with others only when it is legally appropriate to do so
   - Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests
   - Ensure our staff are aware of and understand our policies and procedures

F. Meeting the Data Protection Principles

1) To meet the data protection principles the Academy will:
   - Implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR
   - Provide comprehensive, clear and transparent privacy policies
   - Keep records of activities relating to higher risk processing such as the processing of special categories data or that in relation to criminal convictions and offences
   - Ensure that internal records of processing activities will include the following:
     i) Name and details of the organisation
     ii) Purpose(s) of the processing
     iii) Description of the categories of individuals and personal data
     iv) Retention schedules
     v) Categories of recipients of personal data
     vi) Description of technical and organisational security measures
     vii) Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place
   - Continuously create and improve security features.
   - Implement measures to meet the principles covering data minimisation, transparency and pseudonymisation.
   - Use Data protection Impact Assessments, where appropriate, for new or high risk special projects to minimise any potential privacy risks.

G. Data Protection Officer (DPO)

1) A DPO will be appointed in order to:
   - Inform and advise the Academy and its employees about their obligations to comply with the GDPR and other data protection laws
   - Monitor the Academy's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members

2) The Academy will ensure that:
   - Where the duties are covered by an existing employee their duties are compatible with the duties of the DPO and do not lead to conflict of interests
   - The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to academies
   - The DPO will report to the highest level of management at the academy, which is the Headteacher.
   - The DPO will operate independently
   - Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations.

H. Lawful Processing

1) The legal basis for processing data will be identified and documented prior to data being processed.

2) Under the GDPR, data will be lawfully processed under the following conditions:
   - The consent of the data subject has been obtained.
   - Processing is necessary for:
     i) Compliance with a legal obligation
     ii) The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
     iii) For the performance of a contract with the data subject or to take steps to enter into a contract
     iv) Protecting the vital interests of a data subject or another person
     v) 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

3) Sensitive data will only be processed under the following conditions:
   - Explicit consent of the data subject, unless reliance on consent is prohibited by EU law
   - 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

4) 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 on the basis of EU 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 on the basis of EU law or a contract with a health professional.
   - 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 Article 89(1).

I. Consent

1) Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

2) Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

3) Where consent is given, a record will be kept documenting how and when consent was given.

4) The Academy will ensure that consent mechanisms meet the standards of the 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.

5) Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

6) Consent can be withdrawn by the individual at any time

7) The consent of parents will be sought prior to the processing of a student's data, except where the processing is related to preventative or counselling services offered directly to a student.

J. The Right to be Informed – Privacy Notice

1) The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

2) If services are offered directly to a student, the Academy will ensure that the privacy notice is written in a clear, plain manner that the student will understand.

3) The following information will be supplied within the privacy notice:
   - The identity and contact details of the controller, and where applicable, the controller's representative and the DPO.
   - The purpose of, and the legal 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:
     i) Withdraw consent at any time.
     ii) Lodge a complaint with a supervisory authority.

4) 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 and the details of the categories of personal data, as well as any possible consequences of failing to provide the personal data, will be provided.

5) Where data is not obtained directly from the data subject, information regarding the source the personal data originates from and whether it came from publicly accessible sources, will be provided.

6) For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

7) In relation to data that is not obtained directly from the data subject, 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.

K. The Right of Access

1) Individuals have the right to obtain confirmation that their data is being processed.

2) Individuals have 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.

3) The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:
   - passport
   - driving licence
   - utility bills with the current address
   - birth/ marriage certificate
   - P45/P60
   - credit card or mortgage statement

   This list is not exhaustive.

4) Any individual has the right of access to information held about them. However with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. Personal data about a child belongs to that child, and not the child's parents. This is the case even where a child is too young to understand the implications of subject access rights.

   For a parent to make a subject access request, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent. Therefore most subject access requests from parents of students at this school will not be granted without the express permission of the student. Parents at this Academy do not have an automatic right to access their child's educational record. The Academy will decide on a case-by-case basis whether to grant such requests, bearing in mind guidance issued from time to time from the Information Commissioner's Office

5) The Academy will supply a copy of the information free of charge but may make a charge for the provision of information, dependent upon the following:
   - A 'reasonable fee' will be made to comply with requests for further copies of the same information.

6) Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

7) 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

8) All requests will be responded to without delay and at the latest, within one month of receipt.

9) 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.

10) 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.

11) 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.

L. The Right to Rectification

1) Individuals are entitled to have any inaccurate or incomplete personal data rectified. Where the personal data in question has been disclosed to third parties, the Academy will inform them of the rectification where possible.

2) Where appropriate, the Academy will inform the individual about the third parties that the data has been disclosed to.

3) Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

4) Where no action is being taken in response to a request for rectification, 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.

M. The Right to Erasure

1) Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

2) Individuals 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/processed
   - When the individual withdraws their consent
   - 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 student

3) 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 exercise or defence of legal claims

4) As a student 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 student has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

5) 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.

6) 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.

N. The Right to Restrict Processing

1) Individuals have the right to block or suppress the Academy's processing of personal data.
In the event that 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.

2) 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

3) 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.

4) The Academy will inform individuals when a restriction on processing has been lifted.

O. The Right to Data Portability

1) Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

2) Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

3) The right to data portability only applies in the following cases:
   - To personal data that an individual has provided 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

4) Personal data will be provided in a structured, commonly used and machine-readable form.

5) The Academy will provide the information free of charge.

6) Where feasible, data will be transmitted directly to another organisation at the request of the individual.

7) The Academy is not required to adopt or maintain processing systems which are technically compatible with other organisations.

8) 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.

9) 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.

10) 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.

P. The Right to Object

1) The Academy will inform individuals 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.

2) Individuals have the right to object to the following:
   - Processing based on legitimate interests or the performance of a task in the public interest
   - Direct marketing
   - Processing for purposes of scientific or historical research and statistics.

3) 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.

4) Where personal data is processed for direct marketing purposes:
   - 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.

5) 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.
   - Here the processing activity is outlined above, but is carried out online, the Academy will offer a method for individuals to object online.

Q. Privacy by Design and Privacy Impact Assessments

1) A DPIA will be used when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

2) 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

3) Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the Academy's data protection obligations and meeting individuals' expectations of privacy.

4) 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

5) 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 GDPR.

R. Data Breaches

1) 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.

2) The Headteacher will ensure that all staff members are made aware of, and understand, what constitutes as a data breach as part of their continuous development training.

3) Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

4) All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the Academy becoming aware of it.

5) 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.

6) In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the Academy will notify those concerned directly.

7) A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

8) In the event that a breach is sufficiently serious, the public will be notified without undue delay.

9) 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.

10) Within a breach notification, 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

11) Failure to report a breach when required to do so will result in a fine, as well as a fine for the breach itself.

S. Data Security

1) Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

2) Confidential paper records will not be left unattended or in clear view anywhere with general access.

3) Paper copies of data or personal information should not be taken off the school site. If these are misplaced they are easily accessed. If there is no way to avoid taking a paper copy of data off the school site, the information should not be on view in public places, or left unattended under any circumstances.

4) Unwanted paper copies of sensitive information or student files should be shredded. This also applies to handwritten notes if the notes reference any other staff member or student by name.

5) Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.

6) If information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers.

7) Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

8) Where data is saved on removable storage or a portable device, the device will be kept safe when not in use.

9) Memory sticks will not be used unless they are password-protected and fully encrypted.

10) Data stored on memory sticks should not be transferred from this stick onto any home computer. Work should be edited from the USB and saved onto the USB only.

11) All electronic devices are password-protected to protect the information on the device in case of theft.

12) Where possible, the Academy enables electronic devices to allow the remote blocking or deletion of data in case of theft.

13) Staff will not store personal data on personal laptops or computers.

14) All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password 0n a 4 month cycle.

15) Emails containing sensitive or confidential information in attachments are password-protected and the e mail encrypted if there are unsecure servers between the sender and the recipient.

16) Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

17) When sending confidential information by fax, staff will always check that the recipient is correct before sending.

18) Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the Academy premises accepts full responsibility for the security of the data.

19) Before sharing data, all staff members will ensure:
    - They are allowed to share it.
    - That adequate security is in place to protect it.
    - Who will receive the data has been outlined in a privacy notice.

20) Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the Academy containing sensitive information are supervised at all times.

21) The physical security of the Academy's buildings and storage systems, and access to them, is reviewed on a regular basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

22) The Academy takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

23) The Data Protection Officer is responsible for ensuring continuity and recovery measures are in place to ensure the security of protected data.

T. Publication of Information

1) The Academy will publish a publication scheme on its website outlining classes of information that will be made routinely available, including:
    - Policies and procedures
    - Annual reports
    - Financial information

2) Classes of information specified in the publication scheme are made available quickly and easily on request.

3) The Academy will not publish any personal information, including photos, on its website without the permission of the affected individual.

4) 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.

U. CCTV and Photography

1) The Academy understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

2) The Academy notifies all pupils, staff and visitors of the purpose for collecting CCTV images via the privacy notice or letters and email.

3) Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

4) All CCTV footage will be kept for six months for security purposes; the Data Protection Officer is responsible for keeping the records secure and allowing access.

5) The Academy will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them.

6) Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR

V. Data Retention and Disposal

1) Data will not be kept for longer than is necessary.

2) The Academy policy on data retention is listed in a separate document appended to this policy.

W. DBS Data

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

2) Data provided by the DBS will not be duplicated.

3) 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.