General Data Protection Regulation Policy

Reviewed: August 2019
Next Review: August 2020

Contents

GENERAL DATA PROTECTION REGULATIONS

1.0 STATEMENT OF INTENT

1.1
The Appleby Heritage Centre is committed to protecting the rights and privacy of individuals in accordance with its legal obligations under the General Data Protection Regulation (GDPR).

1.2
AHC is required to keep and process certain information about its learners, staff and other individuals for various purposes such as:

- To support learning;
- To monitor and report on learner progress;
- To provide appropriate pastoral care
- To assess the quality of our services
- To ensure we operate efficiently and effectively
- To recruit and pay staff
- To collect payments
- To comply with legal obligations to funding bodies, lead contract holders and the government
- To enable financial modelling and planning
- To develop a comprehensive picture of the workforce and how it is deployed.

1.3
The centre may be required to share personal information about its employees or learners with other schools, organisations, the LA and social services for example.

1.4
This policy applies to computerised systems and manual records, where personal information is accessible by specific criteria, chronologically or as pseudonymised data, e.g. key-coded. It also applies to photographs, CCTV footage and audio and video systems.

2.0 LEGAL FRAMEWORK

2.1
This policy has due regard to legislation, including, but not limited to the following:

- General Data Protection Regulation (GDPR)
- Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998

2.2
This policy also has regard to the following guidance:

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'

Reviewed: August 2019
Next Review: August 2020

3.0 ASSOCIATED POLICIES

3.1
This policy will be implemented in conjunction with the following policies and procedures:
CCTV Procedures
Internet Access Policy

4.0 DEFINITIONS

4.1
‘Personal data’ refers to any information that relates to an identifiable, living individual (‘data subject’). This could include information such as names, addresses, telephone numbers, photographs, expressions of opinions about an individual or an online identifier (e.g. IP address)

4.2
‘Special categories of personal data’ refers to information which is broadly the same as 'sensitive personal data' previously referred to in the Data Protection Act (DPA) 1998. This includes biometric data, ethnicity, religious beliefs, data concerning health matters and actual or alleged criminal activities.

4.3
‘Processing’ refers to any operation which is performed on personal data such as: collection, recording, organisation, storage, alteration, retrieval, use, disclosure, dissemination or otherwise making available, combination, restriction, erasure or destruction.

4.4
‘Data controller’ refers to any individual or organisation who controls personal data, in this instance The Appleby Heritage Centre Ltd.

4.5
‘Data subject’ refers to an individual who is the subject of the personal data, for example:
- Employees (current and former)
- Learners (including former learners)
- Recruitment applicants (successful and unsuccessful)
- Agency workers (current and former)
- Casual workers (current and former)
- Contract workers (current and former)
- Volunteers (including trustees) and those on work placements
- Claimants and contractors.

5.0 COMPLIANCE

5.1
Compliance with this policy is the responsibility of all the members of AHC who process personal data (including trustees).

5.2
Any breach of this policy may result in disciplinary procedures being invoked. A serious or deliberate breach could lead to dismissal.

Reviewed: August 2019
Next Review: August 2020

5.3
Personal information will only be shared where it is lawful to do so and the third party agrees to abide by this policy and complies with the principles of GDPR.

5.4
This policy will be updated, as necessary, to reflect best practice in data management, security and control and to ensure compliance with any change or amendment to the GDPR and any other relevant legislation.

6.0 DATA PROTECTION PRINCIPLES

6.1
In accordance with article 5 of the GDPR, personal data will be:

- Process lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
- Accurate and, where necessary, kept up to date; ensuring that inaccurate personal data is erased or rectified without delay.
- Kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the personal data is processed.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage.

6.2
AHC will only process personal data in accordance with individuals' rights and will comply with article 5 of the GDPR in the following ways:

- By making all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the identity of the data controller; the purpose of the processing; any disclosures to third parties that are envisaged; an indication of the period for which the data will be kept, and any other information which may be relevant.
- By ensuring that the reason(s) for which the personal data was originally collected is the only reason for which it is processed, unless the individual is informed of any additional processing before it takes place.
- By not seeking to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this in mind. If any irrelevant data is given by individuals, it will be destroyed immediately.
- By reviewing and updating personal data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate. Individuals must notify the centre if a change in circumstances means that their data needs to be updated. It is the responsibility of the centre to ensure that any notification regarding a change is acted on swiftly.
- By undertaking not to retain personal data for longer than is necessary to ensure compliance with the legislation, any other statutory requirement and our Document Retention Records. The centre will undertake a regular review of the information held, both hard copy and electronic.
- By disposing of any personal data in a way that protects the rights and privacy of the individual concerned.

- By ensuring appropriate technical and organisational measures are in place against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of data.

6.3
Personal data may be stored for longer periods and may be processed solely for archiving in the public interest, scientific or historical research, or statistical purposes.

7.0 ACCOUNTABILITY

7.1
The Appleby Heritage Centre Ltd is the registered Data Controller with the Information Commissioner's Office (ICO) and is responsible for controlling the use and processing the personal data it has collected.

7.2
The Appleby Heritage Centre Ltd will implement technical and organisational measures to demonstrate that data is processed in line with the principles set out in this policy. This will include:
- Providing comprehensive, clear and transparent privacy notices
- Using data protection impact assessments (DPIA), where appropriate
- Recording activities relating to higher risk processing, such as the processing of special categories of personal data.

7.3
The privacy notices explain how AHC will share personal data with third parties. This will only occur following consent from the Data Protection Officer (DPO). The sharing of personal data is generally limited to enabling the centre to perform its statutory duties or in respect to a learner`s health, safety and welfare.

7.4
Internal records of processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

7.5
Individuals who provide personal data to AHC are responsible for ensuring that the information is accurate and up to date.

8.0 DATA PROTECTION OFFICER (DPO)

8.1
The DPO for AHC will:

- Inform and advise AHC personnel about their obligations under the GDPR and this policy (including recognising a subject access request, data security and off site use).
- Ensure everyone is aware of and understands, what constitutes a data breach.
- Provide training on GDPR and develop and encourage best practice in the centre.
- Liaise with any external data controllers engaged with AHC.
- Monitor internal compliance, including identifying processing activities and checking the recording of activities related to higher risk processing, advising and checking DPIA's (including need, methodology and any safeguards) and conducting internal audits.
- Take responsibility for continuity and recovery measures to ensure the security of personal data.
- Ensure obsolete personal data is property erased and retain a Destruction Log. This will include the document description, classification, date of destruction, method and authorisation.
- Be the point of contact with the ICO, co-operate with any requests and ensure that the centres notification is kept accurate.
- Maintain an up-to date knowledge of data protection law in relation to organisations

8.2
The DPO will report to the Centre Manager and provide an annual report with recommendations to the Governors.

9.0 LAWFUL PROCESSING

9.1
Personal data will be lawfully processed under the following conditions:
- The consent of the individual has been obtained.
- Compliance with a legal obligation.
- The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- The performance of a contract with the individual or to take steps to enter into a contract.
- Protecting the vital interests of an individual or another person.

9.2
Special categories of personal data will be lawfully processed under the following conditions:

- Explicit consent of the data subject has been obtained, unless reliance on consent is prohibited by EU or Member State 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 individual.
- Carrying out obligations under employment, social security or social protection law, or a collective agreement.
- Protecting the vital interests of an individual or another person where the individual 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 Union or Member State 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 Union or Member State law or a contract with a health professional.
- Reasons of public interest in the area of public health
- Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

9.3
AHC collects and uses workforce information for general purposes under paragraphs 9.1c and 9.2g of this policy which complies with Articles 6 and 9 of the GDPR. Under any other circumstances the legal basis for processing data will be identified and documented prior to data being processed.

10.0 CONSENT

10.1
It is not always necessary to gain consent before processing personal data (see paragraph 9.1 and 9.2) but when it is, consent must be a positive indication.

10.2
Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wished (it cannot be inferred from silence, inactivity or pre-ticked boxes). Consent obtained on the basis of misleading information will not be a valid basis for processing.

10.3
Any forms used to gather personal data will be provided with a privacy notice and will indicate whether or not the individual needs to give consent for the processing.

10.4
A record will be kept documenting how and when consent was given.

10.5
If an individual does not give their consent for processing and there is no other lawful basis on which to process the data, then AHC will ensure that the processing of that data does not take place.

10.6
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.

10.7
Consent can be withdrawn by the individual at any time.

10.8
Parental consent will be sought prior to the processing of a child's data which would require consent until the age of 16, except whether the processing is related to preventative or counselling services offered directly to a child.

10.9

Consent will be sought from the child after the age of 16 if we consider they have the competence to consent for themselves. If there is any doubt parental consent will continue to be required.

11.0 THE RIGHT TO BE INFORMED

11.1
Privacy notices regarding the processing of personal data will be concise, written in clear, accessible language and be free of charge.

11.2
If services are offered directly to a learner, the privacy notice will be written in a way that the learner will understand. This is particularly relevant if this relates to a young person or a person with a learning difficulty or disability.

11.3
AHC will include the following information in its privacy notices following the ICO code of practice:

- The identity and contact details of the controller and the DPO.
- The intended 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 to whom the personal data will be disclosed.
- Details of transfers to third countries and the safeguards in place.
- The retention period or criteria used to determine the retention period.
- The existence of the right to access, rectification, object, erasure and withdraw consent.
- The right to complain internally and to a supervisory authority.

11.4
Where data is obtained directly from an individual, 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 at the time of collection.

11.5
Where personal data about an individual has been obtained indirectly, information regarding the source of the data and whether it was publicly accessible 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 is disclosed.
- If the data is used to communicate with the individual, at the latest, when the first communication takes place.

12.0 THE RIGHT TO ACCESS

12.1
Individuals have the right to obtain confirmation that their data is being processed or to submit a subject access request (SAR) to gain access to their personal data. In order to ensure individuals received the correction information SAR’s must be made in writing and submitted to the Centre Manager at AHC

12.2

The Centre Manager at AHC will verify the identity of the person making the request before any information is supplied.

12.3
All requests will be responded to within one month of receipt.

12.4
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.

12.5
Where a fair processing request is made the information contained with the relevant privacy notice will be provided.

12.6
Where a SAR is made copies of personal data will generally be encrypted and supplied to the individual in a commonly used electronic format.

12.7
Where a SAR is received from a young learner, the centre's policy is that:
- It will be processed in the same way as any other SAR. The information will be given directly to the young learner, unless it is clear that the young learner does not understand the nature of the request.
- Where a young learner does not appear to understand the nature of the request this will be referred to their parents or carers.
- A SAR from parents in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the information will be sent either in a sealed envelope or electronically to the requesting parent.

12.8
In the event that a large quantity of information is being processed the individual may be requested to specify the information the request is in relation to.

12.9
Where a request is excessive or repetitive, a 'reasonable fee' will be charged. All fees will be based on the administrative cost of providing the information.

12.10
Where a request is manifestly unfounded AHC holds the right to refuse to respond to the request. The individual will be informed of this decision and the reason behind it, as well as their right to complaint to the supervisory authority.

13.0 THE RIGHT TO RECTIFICATION

13.1
Personal data held by AHC will be as accurate as is reasonably possible.

13.2

Individuals are entitled to have any inaccurate or incomplete personal data rectified. Where an individual informs AHC of inaccurate or incomplete personal data their data record will be updated as soon as is practicable.

13.3
Where the personal data in question has been disclosed to third parties, the centre will inform them of any rectification where possible. The individual will also be informed about the third parties that the data has been disclosed to where appropriate.

13.4
Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

13.5
Where no action is being taken in response to a request for rectification, AHC 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.

14.0 THE RIGHT TO ERASURE

14.1
Individuals have the right to request erasure of personal data. This applies where:
- Personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- Withdrawal of consent and no other legal ground applies.
- The individual objects to the processing and there is no overriding legitimate interest.
- Personal data is unlawfully processed.
- Personal data has to be erased in order to comply with a law.
- Personal data of a learner is processed in relation to an online service.

14.2
The centre has the right to refuse a request for erasure where the personal data is being processed for:

- Exercising the right of freedom of expression and information.
- Compliance with legal obligations or for performing tasks carried out in the public interest or in exercising the data controller's official authority.
- For public health purposes in the area of public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

14.3
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.

14.4

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.

14.5
Where personal data has been made public and then is requested to be erased, taking into account the available technology and the cost of implementation, all reasonable steps will be taken to inform other data controllers about the request for erasure.

15.0 THE RIGHT TO RESTRICT PROCESSING

15.1
Individuals have the right to restrict the centre's processing of personal data.

15.2
In the event that processing is restricted, the centre 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.

15.3
The centre 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 centre has verified the accuracy of the data
- Where an individual has objected to the processing and the centre 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 centre no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

15.4
If the personal data in question has been disclosed to third parties, the centre will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

15.5
The centre will inform individuals when a restriction on processing has been lifted.

16.0 THE RIGHT TO DATA PORTABILITY

16.1
Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

16.2
Personal data can be moved, copied or transferred from one IT system to another in a safe and secure manner, without hindrance to usability.

16.3
The right to data portability only applies in the following cases:

- Where personal data has been provided by an individual to AHC
- 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

16.4
AHC will respond to any requests for portability within one month and will provide the personal data free of charge and in a structured and commonly used form.

16.5
Where feasible, data will be transmitted directly to another organisation at the request of the individual. AHC is not required to adopt or maintain processing systems which are technically compatible with other organisations.

16.6
In the event that the personal data concerns more than one individual, AHC will consider whether providing the information would prejudice the rights of any other individual.

16.7
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 receipt of the request.

16.8
Where no action is being taken in response to a request AHC will, without delay and at the latest within one month, explain the reason for this. The individual will also be informed of their right to complain to the supervisory authority and to a judicial remedy.

17.0 THE RIGHT TO OBJECT

17.1
AHC will inform individuals of their right to object at the first point of communication. This information will be outlined in privacy notices.

17.2
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.

17.3
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.
AHC will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the centre can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

17.4

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, AHC is not required to comply with an objection to the processing of the data.

18.0 PRIVACY BY DESIGN

18.1
AHC will act in accordance with the GDPR by adopting a 'privacy by design' approach and implementing technical and organisational measures which demonstrate how AHC has considered and integrated data protection into processing activities.

18.2
Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with data protection obligations and meeting individuals' expectations of privacy.

18.3
DPIAs will allow AHC to identify and resolve problems at an early stage, thus preventing reputational damage which might otherwise occur.

18.4
All DPIAs will 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

18.5
A DPIA will be used for new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

18.6
A DPIA will be used for more than one project, where necessary.

18.7
High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences

18.8
Where a DPIA indicates high risk data processing, AHC will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

19.0 DATA BREACH NOTIFICATION

19.1
The term ‘data breach’ refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

19.2
Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

19.3
All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of AHC becoming aware of it.

19.4
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.

19.5
In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, AHC will notify those concerned directly. A ‘high risk’ breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

19.6
In the event that a breach is sufficiently serious, the public will be notified without undue delay.

19.7
Effective and robust breach detection, investigation and internal reporting procedures are in place, which will guide decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

19.8
Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including categories, 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.

19.9
Failure to report a breach when required to do so will result in a fine, as well as a fine for the breach itself.

20.0 DATA SECURITY

20.1
AHC undertakes to ensure the security of the personal data it has collected. Personal data will only be accessible to those who have a valid reason for using it.

20.2

All members of AHC (including trustees) are responsible for ensuring that any personal data they hold is kept secure and not disclosed to any unauthorised third party (a data security user checklist is provided for quick reference in Appendix 5).

20.3 PHYSICAL MEASURES

- Premises security measures, such as intruder alarms, CCTV, fencing and safes are in place
- Only authorised persons are allowed to access to the server room
- Discs, tapes and printouts are locked away securely when not in use
- Visitors to AHC are required to sign in and out, wear identification badges and where appropriate, are accompanied.
- Premises security and storage systems are reviewed on a regular basis. If an increased risk in vandalism / theft is identified, extra measures to secure data storage will be put in place.

20.4 TECHNICAL MEASURES

a) Security software is installed on AHC centre networks and electronic devices. This includes:
- Internet filtering and firewall
- Anti-virus
- Email ransom ware detection

b) Data on the centre network drives is password protected and automatically backed up off-site. There are procedures in place to access and restore all the data held on the centre network drives should this be necessary.

c) AHC electronic devices are password protected and where possible have been enabled to allow remote blocking or deletion of personal data in the case of theft.

d) Centre users are given a secure user name and password to access the centre networks, drives and any other platform they require access to.

e) Password rules are recommended.

f) Centre users will be assigned a clearance that will determine which files are accessible to them. Protected files are not accessible to unauthorised users.

g) Removable storage devices (such as USB sticks) can be used to hold personal data under the following conditions:
- The device **must** be checked by an IT Technician before use;
- It **must** be password protected
- It **must** be stored in a secure and safe place when not in use
- It **must not** be accessed by other users (e.g. family members) when out of centre.
- Personal data **must** be securely deleted when no longer required.

h) Data breach detection tests will be undertaken to evaluate AHC’s technical measures and minimise the chance of data breach.

20.5 ORGANISATIONAL MEASURES

a) Paper records containing personal data **must not** be left unattended or in clear view anywhere with general access.

b) Paper records and removable storage devices **must** be stored in a secure and safe place that avoids physical risk, loss or electronic degradation (exercise books, subject / project folders and worksheets can be stored in classrooms).

c) Paper records containing personal data **must** be kept secure if they are taken off the centre premises.

d) Centre user names and passwords **must** not be shared.

e) Centre electronic devices (such as staff computers) that are used to access personal data **must** be locked even if left unattended for short periods.

f) Computer terminals, CCTV camera screens that show personal data **must** be places so that they are not visible except to authorised staff.

g) Emails **must** be encrypted if they contain personal data.

h) Circular emails must be sent blind copy (bcc) to prevent email addresses being disclosed to other recipients.

i) Visitors **must** not be allowed access to personal data unless they have a legal right to do so or consent has previously been given.

j) Personal data **must** not be given over the telephone unless you are sure of the identity of the person you are speaking to and they have the legal right to request it.

k) Personal data **must** not be disclosed to any unauthorised third parties.

l) Personal electronic devices **must** not be used to hold personal data belonging to AHC.

m) Personal electronic devices **must** be password protected and have up-to-date, active virus and anti-malware checking software before being used to access personal data belonging to AHC via:

- A password protected removable storage device
- Remote access to the centre network
- Any other centre system access

n) Personal electronic devices that have been set to automatically log into the centre network, centre email accounts etc. that are lost or stolen must be reported to the DPO so that access to these systems can be reset.

o) If personal data us taken of AHC premises, in electronic or paper format, extra care **must** be taken to follow the same procedures for security. The person taking the personal data off the centre premises must accept full responsibility for data security.

p) Before sharing personal data, AHC staff and trustees must ensure:

- They are allowed to share it
- That adequate security is in place to protect it

- Who will receive the personal data has been outlines in a privacy notice

q) Any personal data archived on disks **must** be kept securely in a lockable cabinet/archive room.

r) AHC staff must be trained in the application of this policy, their responsibilities and the importance of ensuring data security in order to comply with GDPR.

21.0 CCTV AND PHOTOGRAPHY

21.1
AHC understands that recording images of identifiable individuals constitutes as processing personal data and so is done in compliance with GDPR principles.

21.2
CCTV systems operate on AHC centre premises for the purpose of protecting centre members and property.

21.3
Pupils, staff, parents and visitors are notified of the purpose of collecting CCTV images via signage around the centre premises.

21.4
Cameras are only placed where they do not intrude on an individual's privacy and are necessary to fulfil their purpose.

21.5
CCTV footage is kept for 28 days for security purposed unless it is relevant to an investigation in which case it will be normally kept for a maximum of six months. Detailed guidance is given in the centres CCTV Policy

21.6
AHC may occasionally use photographs / video learners in a publication, such as the centre website, prospectus, and press release.

21.7
Prior to the publication of any photograph or video of learners in the press, social media, centre website or prospectus or in any other marketing or promotional materials, written consent will be sought from parents, as required.

21.8
Photographs or videos captured by other individuals for recreational or personal purposes, such as learners taking photos on a centre trip are exempt from the GDPR.

22.0 DBS DATA

22.1
DBS information is treated as a special category of personal data under this policy.

22.2

DBS information will never be duplicated and any third parties who have lawful access to DBS information will be made aware of their GDPR responsibilities.

23.0 THE SECURE TRANSFER OF DATA

23.1
AHC is required to share personal information with the Department for Education (DfE), Education and Skills Funding Agency (EFSA), Cumbria County Council (CCC), Ofsted, centres and educational institutions, public services and other third party providers. This is a statutory lawful requirement.

23.2
AHC users must not remove copy or share any personal data with a third party without permission from the DPO.

23.3
Where personal data is required to be lawfully shared with a third party it must be securely transferred following encryption, using approved encryption software, and be password protected.

23.4
No personal data will be transferred to a country outside the European Economic Area (EEA) without the explicit consent from the individual. Advice must be taken from the DPO.

24.0 PUBLICATION OF INFORMATION

24.1
A publication scheme can be found on the website. This specifies the classes of information that will be made available on request.

24.2
AHC will not publish any personal data on the centre website without consent from the affected individual(s).

24.3
When uploading information onto the centre websites consideration is given to any metadata or deletions which could be accessed in the documents and images.

25.0 DATA RETENTION

25.1
Personal data will not be kept for longer than is necessary.

25.2
The DPO will ensure that obsolete personal data is properly erased. The length of time we hold personal data is set out in the archive and also Electronic Data Index.

25.3
Personal data that is not required will be deleted as soon as practicable.

Reviewed: August 2019
Next Review: August 2020

25.4
Some educational records relating to former learners or employees may be kept for an extended period of legal reasons, the provision of references or for historical archives.

26.0 DATA DISPOSAL

26.1
AHC will comply with the requirements for the safe destruction and deletion of personal data when it is no longer required.

26.2
Paper documents containing personal data will be shredded or disposed of as 'confidential waste' and appropriate contract terms will be put in place with any third parties undertaking this work.

26.3
Hard drives of redundant PC's and storage devices containing personal data will be securely wiped clean before disposal, or if that is not possible, physically destroyed

26.4
The DPO will retain a Destruction Log of personal data that is disposed of. This will include the document description, classification, date of destruction, method and authorisation.

27.0 TRAINING AND AWARENESS

27.1
AHC users will received GDPR training to make them aware of their responsibilities, this will include methods such as online training, induction training for new staff, staff meetings/briefings/INSET, day to day support and guidance.

28.0 ENQUIRIES

28.1
Any further information, questions or concerns about this policy or the security of data held by AHC should be directed to the DPO (or to the Centre Manager of AHC):

Karen Chester, Data Protection Officer
karen@applebyheritagecentre.org.uk

28.2
General information about GDPR can be obtained from the Information Commissioner's Office.

Reviewed: August 2019
Next Review: August 2020