GDPR &
DATA PROTECTION POLICY

PHASE	JUNIOR & SECONDARY
POLICY LEAD	MARGARET CATLING SENIOR FINANCE OFFICER
DATE OF APPROVAL BY TRUSTEES	29TH APRIL 2019
DATE OF RECEIPT BY LOCAL GOVERNING BODY	MAY 2019
FREQUENCY DATE	EVERY 3 YEARS
REVIEW DATE	MARCH 2022

GDPR and Data Protection Policy

General Data Protection Regulation (GDPR) and The Data Protection Act 2018 (DPA) is the law that protects personal privacy and upholds individual's rights. It applies to anyone who handles or has access to people's personal data.

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the legislation. It will apply to personal information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

Policy Objectives
ACET as the Data Controller will comply with its obligations under the GDPR and DPA. ACET is committed to being concise, clear and transparent about how it obtains and uses personal information and will ensure data subjects are aware of their rights under the legislation.

All staff must have a general understanding of the law and understand how it may affect their decisions in order to make an informed judgement about how information is gathered, used and ultimately deleted. All staff must read, understand and comply with this policy.

The Information Commissioner as the Regulator can impose fines of up to 20 million Euros (approximately £17 million) for serious breaches of the GDPR, therefore it is imperative that ACET and all staff comply with the legislation.

Scope of the Policy
Personal data is any information that relates to an identified or identifiable living individual who can be identified directly or indirectly from the information[1]. The information includes factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a living individual. This includes any expression of opinion about an individual and intentions towards an individual. Under the GDPR personal information also includes an identifier such as a name, an identification number, location data or an online identifier.

ACET collects a large amount of personal data every year including: pupil/student records, staff records, names and addresses of those requesting prospectuses, examination marks, references, fee collection as well as the many different types of research data used by ACET. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies.

The Principles
The principles set out in the GDPR must be adhered to when processing personal data:

1. Personal data must be processed lawfully, fairly and in a transparent manner (**lawfulness, fairness and transparency**)
2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (**purpose limitation**)
3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed (**data minimisation**)
4. Personal data shall be accurate and where necessary kept up to date and every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay (**accuracy**).

[1] GDPR Article 4 Definitions

5. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data is processed (**storage limitation**)
6. Appropriate technical and organisational measures shall be taken to safeguard the rights and freedoms of the data subject and to ensure that personal information are processed in a manner that ensures appropriate security of the personal data and protects against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data (**integrity and confidentiality**).

Transfer Limitation

In addition, personal data shall not be transferred to a country outside the EEA[2] unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data as determined by the European Commission or where the organisation receiving the data has provided adequate safeguards[3].

This means that individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer. It may also be possible to transfer data where the data subject has provided explicit consent or for other limited reasons. Staff should contact the DPO if they require further assistance with a proposed transfer of personal data outside of the EEA.

Lawful Basis for processing personal information

Before any processing activity starts for the first time, and then regularly afterwards, the purpose(s) for the processing activity and the most appropriate lawful basis (or bases) for that processing must be selected:

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in ACET
- Processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract
- Processing is necessary for compliance with a legal obligation to which the data controller is subject
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person
- Processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party[4]
- The data subject has given consent to the processing of his or her data for one or more specific purposes. Agreement must be indicated clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or

[2] Please refer to section 3.1 of the E-SAFETY & DATA PROTECTION policy at www.astoncetrust.org
[3] These may be provided by a legally binding agreement between public authorities or bodies, standard data protection clauses provided by the ICO or certification under an approved mechanism.
[4] The GDPR states that legitimate interests do not apply to processing carried out by public authorities in the performance of their tasks, Article 6 However, the ICO indicates that where there are other legitimate purposes outside the scope of the tasks as a public authority, legitimate interests may be considered where appropriate (particularly relevant for public authorities with commercial interests).

inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, the consent from be kept separate from those other matters

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if personal data is intended to be processed for a different and incompatible purpose which was not disclosed when the data subject first consented.

The decision as to which lawful basis applies must be documented, to demonstrate compliance with the data protection principles and include information about both the purposes of the processing and the lawful basis for it in ACET's relevant privacy notice(s).

When determining whether legitimate interests are the most appropriate basis for lawful processing (only where appropriate outside ACET's public tasks) a legitimate interest assessment must be carried out and recorded. Where a significant privacy impact is identified, a data protection impact assessment (DPIA) may also need to be conducted.

Sensitive Personal Information

Processing of sensitive personal information (known as 'special categories of personal data') is prohibited[5] unless a lawful special condition for processing is identified.

Sensitive personal information is data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life or orientation or is genetic or biometric data which uniquely identifies a natural person.

Sensitive personal information will only be processed if:

- There is a lawful basis for doing so as identified on previous page
- One of the special conditions for processing sensitive personal information applies:
    - (a) the individual ('data subject') has given explicit consent (which has been clearly explained in a Privacy Notice)
    - (b) the processing is necessary for the purposes of exercising the employment law rights or obligations of ACET or the data subject
    - (c) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent
    - (d) the processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim
    - (e) the processing relates to personal data which are manifestly made public by the data subject
    - (f) the processing is necessary for the establishment, exercise or defence of legal claims
    - (g) the processing is necessary for reasons of substantial public interest
    - (h) the processing is necessary for purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, the provision of social care and the management of social care systems or services
    - (i) the processing is necessary for reasons of public interest in the area of public health

ACET's privacy notice(s) set out the types of sensitive personal information that it processes, what it is used for, the lawful basis for the processing and the special condition that applies.

[5] GDPR, Article 9

Sensitive personal information will not be processed until an assessment has been made of the proposed processing as to whether it complies with the criteria above and the individual has been informed (by way of a privacy notice or consent) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

Unless ACET can rely on another legal basis of processing, explicit consent is usually required for processing sensitive personal data. Evidence of consent will need to be captured and recorded so that ACET can demonstrate compliance with the GDPR.

Automated Decision Making
Where ACET carries out automated decision making (including profiling) it must meet all the principles and have a lawful basis for the processing. Explicit consent will usually be required for automated decision making (unless it is authorised by law or it is necessary for the performance of or entering into a contract).

Additional safeguards and restrictions apply in the case of solely automated decision-making, including profiling. ACET must as soon as reasonably possible notify the data subject in writing that a decision has been taken based on solely automated processing and that the data subject may request ACET to reconsider or take a new decision. If such a request is received staff must contact the DPO as ACET must reply within 21 days.

Data Protection Impact Assessments (DPIA)
All data controllers are required to implement 'Privacy by Design' when processing personal data.

This means ACET's processes must embed privacy considerations and incorporate appropriate technical and organisational measures (like pseudonymisation) in an effective manner to ensure compliance with data privacy principles.

Where processing is likely to result in high risk to an individual's data protection rights (for example where a new technology is being implemented) a DPIA must be carried out to assess:

- whether the processing is necessary and proportionate in relation to its purpose
- the risks to individuals
- what measures can be put in place to address those risks and protect personal information

Staff should adhere to the Data Protection Toolkit for Academies from the DfE with reference to the DPIA template.

When carrying out a DPIA, staff should seek the advice of the DPO for support and guidance and once complete, refer the finalised document to the DPO for sign off.

Documentation and records
Written records of processing activities must be kept and recorded including:

- the name(s) and details of individuals or roles that carry out the processing
- the purposes of the processing
- a description of the categories of individuals and categories of personal data
- categories of recipients of personal data
- details of transfers to third countries, including documentation of the transfer mechanism safeguards in place
- retention schedules
- a description of technical and organisational security measures

As part of ACET's record of processing activities the DPO will document, or link to documentation on:

- information required for privacy notices
- records of consent
- controller-processor contracts
- the location of personal information;
- DPIAs and
- Records of data breaches.

Records of processing of sensitive information are kept on:

- The relevant purposes for which the processing takes place, including why it is necessary for that purpose
- The lawful basis for our processing and
- Whether the personal information is retained or erased in accordance with the Retention Schedule and, if not, the reasons for not following the policy.

ACET should conduct regular reviews of the personal information it processes and update its documentation accordingly. This may include:

- Carrying out information audits to find out what personal information is held
- Talking to staff about their processing activities
- Reviewing policies, procedures, contracts and agreements to address retention, security and data sharing.

Privacy Notice

ACET will issue privacy notices as required, informing data subjects (or their parents, depending on age of the pupil/student, if about pupil/student information) about the personal information that it collects and holds relating to individual data subjects, how individuals can expect their personal information to be used and for what purposes.

When information is collected directly from data subjects, including for HR or employment purposes, the data subject shall be given all the information required by the GDPR including the identity of the data controller and the DPO, how and why ACET will use, process, disclose, protect and retain that personal data through a privacy notice (which must be presented when the data subject first provides the data).

When information is collected indirectly (for example from a third party or publicly available source) the data subject must be provided with all the information required by the GDPR as soon as possible after collecting or receiving the data. ACET must also check that the data was collected by the third party in accordance with the GDPR and on a basis which is consistent with the proposed processing of the personal data.

ACET will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

ACET will issue a minimum of two privacy notices, one for pupil/student information, and one for workforce information, and these will be reviewed in line with any statutory or contractual changes.

These privacy notices can be found at: **www.astoncetrust.org**

Purpose Limitation
Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

Personal data must not be used for new, different or incompatible purposes from that disclosed when it was first obtained unless the data subject has been informed of the new purposes and they have consented where necessary.

Data minimisation
Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

Staff may only process data when their role requires it. Staff must not process personal data for any reason unrelated to their role.

ACET maintains a Retention Schedule to ensure personal data is deleted after a reasonable time for the purpose for which it was being held, unless a law requires such data to be kept for a minimum time. Staff must take all reasonable steps to destroy or delete all personal data that is held in its systems when it is no longer required in accordance with the schedule. This includes requiring third parties to delete such data where applicable.

Staff must ensure that data subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

Individual Rights
Staff as well as any other 'data subjects' have the following rights in relation to their personal information:

- To be informed about how, why and on what basis that information is processed *(see the relevant privacy notice)*

- To obtain confirmation that personal information is being processed and to obtain access to it and certain other information, by making a subject access request to: - datacontroller@astoncetrust.org

- To have data corrected if it is inaccurate or incomplete

- To have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing ('the right to be forgotten')

- To restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased) or where ACET no longer need the personal information, but you require the data to establish, exercise or defend a legal claim

- To restrict the processing of personal information temporarily where you do not think it is accurate (and ACET are verifying whether it is accurate), or where you have objected to the processing (and ACET are considering whether ACET's legitimate grounds override your interests)

- In limited circumstances to receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format

- To withdraw consent to processing at any time (if applicable)
- To request a copy of an agreement under which personal data is transferred outside of the EEA.
- To object to decisions based solely on automated processing, including profiling
- To be notified of a data breach which is likely to result in high risk to their rights and obligations
- To make a complaint to the ICO or a Court

See Appendix 1 for the procedure for making a subject access request

Individual Responsibilities
During their employment, staff may have access to the personal information of other members of staff, suppliers, clients or the public. ACET expects staff to help meet its data protection obligations to those individuals.

If you have access to personal information, you must:

- only access the personal information that you have authority to access and only for authorised purposes
- only allow other staff to access personal information if they have appropriate authorisation
- only allow individuals who are not Trust staff to access personal information if you have specific authority to do so
- keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction in accordance with ACET's policies)
- not remove personal information, or devices containing personal information (or which can be used to access it) from ACET's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device
- not store personal information on local drives or on personal devices that are used for work purposes

Information Security
ACET will use appropriate technical and organisational measures to keep personal information secure, to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

All staff are responsible for keeping information secure in accordance with the legislation and must follow their academy's acceptable usage policy.

ACET will develop, implement and maintain safeguards appropriate to its size, scope and business, its available resources, the amount of personal data that it owns or maintains on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). It will regularly evaluate and test the effectiveness of those safeguards to ensure security of processing.

Staff must guard against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. Staff must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure.

Staff must follow all procedures and technologies put in place to maintain the security of all personal data from the point of collection to the point of destruction. Staff may only transfer personal data to third-party service providers who agree in writing to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

Staff must maintain data security by protecting the **confidentiality, integrity and availability** of the personal data, defined as follows:

Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it.

Integrity means that personal data is accurate and suitable for the purpose for which it is processed.

Availability means that authorised users can access the personal data when they need it for authorised purposes.

Staff must comply with and not attempt to circumvent the administrative, physical and technical safeguards the academy has implemented and maintains in accordance with the GDPR and DPA.

Where ACET uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. Contracts with external organisations must provide that:

- the organisation may only act on the written instructions of ACET
- those processing data are subject to the duty of confidence
- appropriate measures are taken to ensure the security of processing
- sub-contractors are only engaged with the prior consent of ACET and under a written contract
- the organisation will assist ACET in providing subject access and allowing individuals to exercise their rights in relation to data protection
- the organisation will delete or return all personal information to ACET as requested at the end of the contract
- the organisation will submit to audits and inspections, provide ACET with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell ACET immediately if it does something infringing data protection law

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval from the DPO.

Storage and retention of personal information
Personal data will be kept securely in accordance with ACET's data protection obligations.

Personal data should not be retained for any longer than necessary. The length of time data should be retained will depend upon the circumstances, including the reasons why personal data was obtained. Personal information that is no longer required will be deleted in accordance with ACET's Record Retention Schedule.

See Appendix 2 for ACET's Record Retention Schedule

Data breaches
A data breach may take many different forms:

- Loss or theft of data or equipment on which personal information is stored
- Unauthorised access to or use of personal information either by a member of staff or third party
- Loss of data resulting from an equipment or systems (including hardware or software) failure
- Human error, such as accidental deletion or alteration of data
- Unforeseen circumstances, such as a fire or flood
- Deliberate attacks on IT systems, such as hacking, viruses or phishing scams
- Blagging offences where information is obtained by deceiving the organisation which holds it

ACET must report a data breach to the Information Commissioner's Office (ICO) without undue delay and where possible within 72 hours, if the breach is likely to result in a risk to the rights and freedoms of individuals. ACET must also notify the affected individuals if the breach is likely to result in a high risk to their rights and freedoms.

Staff should ensure they inform their line manager/DPO/Principal immediately that a data breach is discovered and make all reasonable efforts to recover the information, following ACET's agreed breach reporting process at **www.astoncetrust.org**

See Appendix 3 for the step by step guide for what to do in the event of a data breach.

Training
ACET will ensure that staff are adequately trained regarding their data protection responsibilities.

Consequences of a failure to comply
ACET takes compliance with this policy very seriously. Failure to comply puts data subjects whose personal information is being processed at risk and carries the risk of significant civil and criminal sanctions for the individual and ACET and may in some circumstances amount to a criminal offence by the individual.

Any failure to comply with any part of this policy may lead to disciplinary action under the academy's procedures and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

If you have any questions or concerns about this policy, you should contact your line manager or ACET's DPO.

Review of Policy
This policy will be updated as necessary to reflect best practice or amendments made to the GDPR or DPA.

The Supervisory Authority in the UK
Please follow this link to the ICO's website (https://ico.org.uk/) which provides detailed guidance on a range of topics including individuals' rights, data breaches, dealing with subject access requests, how to handle requests from third parties for personal data etc.

Glossary

Automated Decision-Making (ADM): when a decision is made which is based solely on automated processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits automated decision-making (unless certain conditions are met) but not automated processing.

Automated Processing: any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of automated processing.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, which signifies agreement to the processing of personal data relating to them.

Data Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. It is responsible for establishing practices and policies in line with the GDPR. ACET is the Data Controller of all personal data relating to its pupils/students, parents and staff.

Data Subject: a living, identified or identifiable individual about whom we hold personal data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their personal data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major systems or business change programs involving the processing of personal data.

Data Protection Officer (DPO): the person required to be appointed in public authorities under the GDPR.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

Explicit Consent: consent which requires a very clear and specific statement (not just action).

General Data Protection Regulation (GDPR): General Data Protection Regulation (*(EU) 2016/679*). Personal data is subject to the legal safeguards specified in the GDPR.

Personal data is any information relating to an identified or identifiable natural person (data subject) who can be identified, directly or indirectly by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal data includes sensitive personal data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Notices: separate notices setting out information that may be provided to Data Subjects when ACET collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, Trust workforce privacy policy) or they may be stand-alone privacy statements covering processing related to a specific purpose.

Processing means anything done with personal data, such as collection, recording, structuring, storage, adaptation or alteration, retrieval, use, disclosure, dissemination or otherwise making available, restriction, erasure or destruction.

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal data relating to criminal offences and convictions.

Acknowledgement:
This policy and appendices are adapted from Derbyshire County Council policy and procedures

Appendix 1

Subject Access Requests (SAR)

Updated to take into account ICO audit actions, Data Protection Act 2018 and GDPR.

This document has been prepared using the following ISO27001:2013 standard controls as reference:

ISO Control Description
A.18.1.1 Identification of applicable legislation and contractual requirements
A.18.1.3 Protection of records
A.18.1.4 Privacy and Protection of personally identifiable information

Introduction
The General Data Protection Regulation(GDPR) and the Data Protection Act 2018 (the Act) give individuals a number of rights, including a right to obtain a copy of their personal data as well as other supplementary information. This right of access, is often referred to as a right of "subject access". It helps individuals understand how and why you are using their data, and check you are doing it lawfully.

In addition to rights in relation to accessing their data the Data Protection Act 2018 and GDPR give individuals a number of additional rights including the right to rectification (correction of inaccurate data), the right to erasure (sometimes referred to as the right to be forgotten), the right to restrict processing and the right to object to the processing of their data.

Requests for information in accordance with the Data Protection Act 2018 differ from requests for information under the Freedom of Information Act 2000 by virtue of the fact that the information identifies the requester and is about them personally.

Under the Act, ACET has a legal obligation to provide a copy of the data to the requester without undue delay and at the latest within one month of receipt. If the request is particularly complex, or repeated, in some cases it is possible to extend the period by a further two months.

In addition to receiving their personal data, individuals also have a right to know why you are processing their personal data, the categories of data you are processing, who you share this information with, how long you keep their information for, where it originated from, how it is stored, who they can complain to if they are not happy with the way their information has been handled and how their information is safeguarded. Some of this information is likely to be included in ACET's privacy notices and ACET's retention schedules at www.astoncetrust.org

This procedure details the way in which ACET should process a SAR request; a step by step procedure is followed by more detailed guidance notes to assist officers responsible for processing requests of this kind. The Information Commissioner's Office also produces helpful guidance which is regularly updated and will assist in ensuring that ACET is following best practice. Please see the following link: https://ico.org.uk

Recognising a request

A template request form is available to assist individuals in making a request and also ACET locating the relevant information. However, whilst we may invite individuals to use the template form, it is not compulsory and requests made by letter, email or verbally must still be responded to. This form can be found at www.astoncetrust.org

The GDPR does not specify how to make a valid request. Therefore, unlike under the previous Data Protection Act, a request does not have to be in writing it can be made verbally. It can also be made to any part of ACET (including via social media).

A request does not have to include any specific wording such as, 'subject access request', it just has to be clear that the individual is asking for their own personal data.

On receipt of a request for personal information it will be determined whether this is formal Subject Access Request or day to day operational requirements.

For example, we would not automatically consider a student request for a copy of their monitoring report or a staff request for their teacher reference number to be a formal SAR. This type of informal request would not fall under the remit of ACET's SAR procedures unless specified by the individual, however would be compliant under current GDPR and Data Protection legislation.

What is an individual entitled to?
Individuals have the right to obtain the following:

- Confirmation that you are processing their personal data and the legal basis for the processing
- The categories of personal data concerned
- The recipients or categories of recipients to whom their personal information has been disclosed
- Details of how long their information will be kept
- Any information held relating to the origin of their personal data
- A copy of their personal data; and
- Confirmation of their right to lodge a complaint with the Information Commissioner.

The deadline for responding will be calculated from the day following receipt (whether this is a working day or not) so it is important to ensure that it is forwarded as soon as possible to the relevant departmental contact.

How information should be provided
If an individual makes a request electronically, where possible you should provide the information in a commonly used electronic format, unless the individual requests otherwise.

Can I charge a fee for responding to a request?
In most cases you cannot charge a fee to comply with a subject access request. However, where the request is manifestly unfounded or excessive you may charge a "reasonable fee" or the administrative costs of complying with the request. You can also charge a reasonable fee if an individual requests further copies of their data following a request. You must base the fee only on the administrative costs of providing further copies. You should seek guidance from the DPO if you are considering charging a fee.

What happens if information changes from the time of the request?

The Information Commissioner's view is that a subject access request relates to data held at the time the request was received. However, in some cases routine use of data may result in it being amended, or even deleted during the time you are dealing with the request.

In these circumstances it would be reasonable to supply information you hold at the time you send out the response, even if this is different to material held when the request was received. You must not amend, or delete data relevant to the request if you would not otherwise have done so. Under the Data Protection Act 2018, it is an offence to make any amendment to information held with the intention of preventing disclosure.

When information should be provided

You must act on the subject access request without undue delay and at the latest within one month of receipt. You should calculate the time limit from the day after you receive the request (this includes weekends and bank holidays), until the corresponding calendar date in the next month. If this is not possible e.g. the following month is shorter and there is therefore no corresponding calendar date, the date for response is the last day of the following month. If the corresponding date is a weekend or bank holiday, ACET has until the following working day to respond. This means that the exact number of days will vary between requests. For reasons of administrative convenience, you may calculate the deadline on the basis of a 28 day period to ensure your compliance date is always within a calendar month.

Extending time limits
It is possible to extend the time to respond by a further two months if the request is complex or ACET has received a number of requests from the same individual. You must let the individual know within one month of receiving their request if you intend to extend the time limit in respect of their request and you must explain to them why the extension is necessary.

Data Breaches
The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. Where feasible, this must be done within 72 hours of becoming aware of the breach. A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data e.g. it could include an unauthorised individual accessing records or emails containing personal data to the wrong recipient. If you suspect that there has been a data breach you should inform your line manager as soon as possible.

Further information relating to data breaches can be found at www.astoncetrust.org

Step by step procedure

A request for personal information, which is deemed to be an SAR is received. If the request is made verbally a written note of the request should be taken and verified with the requester. The request is emailed to the DPO for processing at datacontroller@astoncetrust.org

1. The DPO (or nominated representative) logs the request.
2. The DPO (or nominated representative) considers whether it is necessary to verify the requester's identity.
3. The DPO (or nominated representative) considers whether they have enough information to locate the required data or whether it is necessary to seek further clarification from the requester.

4. After giving due consideration at steps 3 and 4 the DPO (or nominated representative) is in a position to acknowledge the request in writing. A standard letter acknowledging the request will be modified as appropriate depending on whether the DPO (or nominated representative) requires further clarification and/ or proof of identity.
5. The DPO (or nominated representative) calculates the time limit for responding to the request and logs this. The request should be responded to without undue delay and at the latest within one month of receipt, unless it is necessary to extend the time limit due to the request being complex or repeated. If the time limit is to be extended the requester must be notified of the reasons for this within 1 month of their initial request.
6. The DPO (or nominated representative) ensures that all of the personal data which is relevant to the request is gathered, either by collecting the information himself/ herself or by liaising with the appropriate Academy officer/s.
7. After all of the information has been gathered, the officer preparing the information must ensure at this stage that third party data is redacted or the appropriate consents are sought and that all other information is removed or redacted as appropriate.
8. An electronic copy must be retained of all of the information that was considered in response to the request in an unredacted format as well as the redacted version. It is very important that it is clear what information has been withheld and which exemption has been engaged. The Departments will have their own procedure for ensuring the information is stored in a convenient location either by the DPO (or nominated representative) or the officer preparing the information.
9. When the information has been prepared and has been recorded as stipulated at point 8, the requester should be informed that the information is ready either to be sent out or to be collected.
10. Depending on the nature of the information, Academies may want to invite the requester to read the records with an officer in order that the requester can discuss any concerns or questions they have about the information. However, in most circumstances the information will simply be sent to the requester's home address. Care should be taken when addressing envelopes and ensuring that it is securely packaged. If information is being supplied via email, the ACET's secure email policy must be followed.
11. The DPO (or nominated representative) must log each completed request.

Step 1 – SAR is received
Individuals often ask for their personal data under the Freedom of Information Act 2000 (FOI). This is not the correct legislation under which to process the subject access requests as the two pieces of legislation are significantly different. It is possible to receive a request for information which should be provided under both regimes and therefore it may be necessary to consider the ACET's response from a FOI perspective too. It is for the officer processing the request to inform the requester of the correct piece of legislation and the time limits that apply. If there is any doubt you should seek further guidance from the DPO (or nominated representative). There are a number of different ways that a SAR can be submitted to ACET. For example; a service user may phone the Academy to make initial enquiries, in which case the Academy may send the enquirer a form to fill out and return to the appropriate DPO (or nominated representative). The DPO (or nominated representative) then follows the steps above. A SAR may be emailed or posted directly to the Academy. Any request by an individual for their personal data is a valid SAR. Regardless of where it is received it must be sent to the DPO (or nominated representative) for processing.

Step 2 – The DPO logs the request on ACET's database.
It is important from a quality assurance perspective to ensure that there is a way of tracking the progress of a particular request in order that officers can be reminded of approaching deadlines and to monitor ACET's record in complying with statutory deadlines. It is also important to ensure that a detailed log is kept to ensure ACET can adequately respond to any complaints made to the Information Commissioner.

Step 3 – The DPO considers whether it is necessary to verify the requester's identity. I
It is the enquirer's responsibility to prove that they are the data subject or that they represent the data subject. It is ACET's responsibility to ensure that requesters are required to provide appropriate proof of identity where this is necessary, before supplying information. It is important that you only ask for information that is necessary to confirm the identity of the requester. It is important to act proportionately; you need to let the individual know as soon as possible if you need more information in order to confirm their identity. The time limit for responding to the request begins from when you received the additional information.

As data controller ACET is entitled to ask for any information that officers may reasonably require to establish the identity of a requester. The DPO (or nominated representative) should work with officers in individual academies to establish whether the Academy is providing services to the requester at the time of the SAR. If services are being provided at the time of the request, it is an 'open case'. Where the DPO (or nominated representative) is satisfied that officers know the identity and correct current address of the requester by virtue of their ongoing relationship with ACET, then there is no need to obtain further proof of identification or address. However, where there is any doubt regarding the address or identity of a requester, they must be asked to supply the documents listed below.

If, upon receipt of the request, or after communication with officers, it is clear that the requester is not receiving services from ACET at the time of the request this is a 'closed case' and more stringent identification requirements must be applied here. It may be reasonable to telephone or write to the requester. The requester must be asked to supply one form of original photo identification along with a utility bill dated within the last three months indicating their current address. A passport, a photographic driving licence, or a bus pass can be used to establish identity and the electoral roll can also be used to confirm postal addresses. Requesters may not want to send their passport or driving licence through the post in which case an appointment should be made by the DPO (or nominated representative) to inspect the document. It is not necessary to retain a copy of the identification document but it is very important that a note is retained to indicate the document has been inspected and approved by the DPO (or nominated representative). Where the requester sends the original through the post, it should be inspected and logged and sent back to the requester via recorded delivery as soon as possible.

Step 4 -The DPO considers whether they have enough information to locate the required data.
Occasionally requesters will make a written request for 'everything ACET holds on me'; in these circumstances it is reasonable to ask for clarification. In these situations, it will be reasonable to write to the requester explaining that you need further information before you can begin to locate the information. You should only ask for information that you reasonably need to find the personal data covered by the request.

If the DPO (or nominated representative) requires further information, it must be requested as soon as possible as delays may have to be justified to the Commissioner at a later date. The period for responding to the request begins when you receive the additional information. However, if an individual refuses to comply and provide additional information the Information Commissioner advises that you must still endeavour to comply with their request i.e. by making reasonable searches for the information covered by the request.

Step 5 – The DPO acknowledges the request in writing.
When acknowledging the initial request, you should confirm the deadline by which you will respond, alternatively if you need identification, a fee, or further information to process the request you should make the requester aware of this as soon as possible and confirm that the response deadline will

be re-calculated once you have this information. If you deem the request complex you must also let the requester know the reasons for this within one month of receipt.

Step 6 – The DPO calculates the date on which the response must be provided
Requests have to be dealt with without undue delay, or within a 1 month (unless complex or repeated). The time limit should be calculated from the earliest of the following days;

- the day following of receipt of the request, if you do not require proof of identity or clarification of what information is required* (see note at step 4), or
- the date upon which you have received all of the information you require in relation to verifying the requesters identity.

Where there are unavoidable delays and it is clear to the DPO (or nominated representative) that the time limit will be exceeded then the DPO (or nominated representative) should write to the requester setting out the reason for the delay and giving the requester an indication of when ACET will be in a position to provide a full response. It may be reasonable to telephone or write to the requester. If some, but not all, information relevant to the request has been obtained then the DPO (or nominated representative) should consider whether any information may be provided to the requester within the time limit, with an assurance that any outstanding information will be provided by a particular date.

Step 7 – the DPO ensures that all of the relevant information is considered.
ACET has a duty to provide a requester with a copy of, or access to all structured personal data held in what is defined by the Act as held in a 'filing system'. This is drafted more widely than the previous Data Protection Act and covers any personal data held by ACET either manually or by automated means wherever it is located. It is only necessary to search for information that has actually been requested. You are not required to produce information which has been destroyed prior to the receipt of a request.

Relevant information should never be destroyed after a request has been received. If you are seeking clarification from the requester to help locate their information it may be helpful to establish:

• where the requester thinks that their information is likely to be held;
• the names of the authors and recipients of any messages;
• the subject line of the e-mails;
• the dates, or range of dates, on which the messages were sent;

After searching central manual and computerised files, the DPO (or nominated representative) may need to send a request to individual Academies asking them to search their own records for information about the individual. Please remember that the purpose of the search is to uncover all the information that we hold, as a Trust about the individual. More detailed searches at this stage are likely to result in fewer queries and complaints afterward. The GDPR requires that the information provided to an individual is in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Essentially, this means that the information provided in response to a request should be capable of being understood by the average person (or a child). If when preparing a response to a subject access request you notice that a lot of information is in coded form which would make it impossible for those outside ACET to understand you should explain the meaning of it. You are not legally required to decipher poorly written notice but as a matter of good practice if possible you should do this.

Step 8 – The information is prepared
There are some types of information that the Act says you do not have to provide when responding to a subject access request such as some information relating to third parties.

Legal advice should be sought if you are not sure whether to apply an exemption. Further detailed guidance in relation to relevant exemptions will be provided in due course. Where the requested information includes personal data relating to another individual (a third party), you need to consider whether to release that information to the enquirer. There are three actions you can take:

1. You can obtain the third party's consent to the disclosure, if it is reasonable to do so, or
2. You can edit the information so as not to reveal the third party's identity, for example, blocking out the text or retyping text without the identifying information; or
3. You can decide that it is reasonable to disclose the information to the data subject without the third party's consent.

In taking this third option you need to consider:

- the type of information you would disclose
- any duty of confidentiality owed to a third party
- any steps you have taken to obtain consent;
- whether the third party is capable of giving consent;
- whether the third party has expressly refused consent;
- whether the information is of particular importance to the data subject.

For the purposes of data protection, references to ACET officers carrying out their professional roles and duties and records of their professional assessments, statements or opinions are not generally considered to be third-party data.

Refusing to comply with a request
You can refuse to comply with a subject access request if it is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

If you consider that a request is manifestly unfounded or excessive you can request a “reasonable fee” to deal with the request or refuse to deal with it. However, in either case you will need to justify your decision and confirm the reasons for this to the requester. If you decided to charge a fee you do not need to comply with the request until this has been received.

Step 10 – Finalising, recording and retaining the progress of the SAR.
It is important that the DPO (or nominated representative) is sent a copy of the response if they are not the officer responsible for preparing the information. The DPO (or nominated representative) will record the request as complete when they have sent the information to the requester or the responding officer has sent the DPO (or nominated representative) a copy of their response. Again, it is important to retain an electronic copy of the information that was considered as well as a copy of any information that was withheld in full or redacted. A clear record should be kept explaining the legal basis upon which each document/ section of the document was withheld.

All correspondence between the DPO (or nominated representative) and the enquirer should also be retained. This is necessary because the information may be needed internally as part of a complaints investigation or audit, or externally, as part of an investigation by the regulator. This information should be retained for one year from the date upon which the information was sent to the requester. Individual Academies will have their own way of ensuring the information described above is recorded. Please note that the regulator, the Information Commissioner, is duty bound by law to investigate any and all complaints made in relation to an organisations handling of personal data. It is important that a request is marked as complete for quality assurance purposes and to allow the DPO (or nominated representative) to chase up overdue requests. DPO’s (or nominated representatives) should maintain records of SAR compliance rates.

Requests made on behalf of others.
Subject access requests can be made on behalf of others e.g. a solicitor may request information on behalf of their client, other individuals may feel more comfortable with the request being made by someone else acting on their instructions. In these cases, you must be satisfied that the third party making the request is entitled to act on behalf of the individual. It is the responsibility of the person making the request to demonstrate that they are making the request on behalf of the individual. This could be via a written authority from the data subject or a power of attorney.

If you think that an individual may not understand what information would be disclosed to a third party who has made a subject access request on their behalf, you may send the information directly to the data subject in order that they can then decide whether to share it once they have had the opportunity to review it.

Other organisations can also make requests for personal data such as the Police, the Inland Revenue, the Audit Commission or a court, these are not Subject Access Requests and are therefore not dealt with under this procedure.

Other institutions can also make requests, such as the Police, the Inland Revenue, the Audit Commission or a court. But these are not Subject Access Requests and therefore should not be processed in accordance with this procedure.

Requests for educational records held by schools.
Different rules apply to educational records and these should also be considered under the Education (Pupil Information) (England) Regulations 2005. The definition of an educational record is wide and includes: any information which is processed by or on behalf of the governing body of, or a teacher at, any school maintained by a local authority and any special school which is not maintained; relates to any person who is or has been a pupil at any such school; originated from or was supplied by or on behalf of any employee of the local authority which maintains the school or former school attended by the pupil to whom the record relates; in the case of a voluntary aided, foundation or foundation special school or a special school which is not maintained by a local authority, a teacher or other employee at the school or at the pupil's former school (including any educational psychologist engaged by the governing body under a contract for services); the pupil to whom the record relates; and a parent of that pupil. It therefore includes the curricular record and also includes:

- Any education, health and care (EHC) plan, formerly a statement of special educational need.
- Any personal education plan

Educational records do not include information which is processed by a teacher solely for the teacher's own use, such as lesson plans.

Requests for information about children
Even if a child is too young to understand the implications of subject access rights, it is still the right of the child to make a request rather than anyone else such as a parent or guardian. In the case of young children, this is likely to be exercised by those with parental responsibility. Before responding to a subject access request for information held about a child, you should consider whether the child is mature enough to understand their rights. If you are confident that a child can understand their rights then you should usually respond directly to the child. When considering borderline cases, you should take into account, amongst other things:

- The child’s level of maturity and their ability to make decisions like this;
- The nature of the personal data;
- Any court orders relating to parental access or responsibility that may apply;

- Any duty of confidence owed to the child or young person;
- Any consequence of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment; Any detriment to the child or young person if individuals with parental responsibility cannot access this information;
- Any views of the child or young person has on whether their parents should have information about them;

If Academies offer an online service directly to children on the basis of consent, then the Data Protection Act 2018 specifies 13 years old as the appropriate age of consent.

Complaints
All complaints about subject access must be immediately notified to the DPO who will determine the appropriate next steps. The DPO should maintain a record of all requests for internal reviews and complaints which are escalated to the Information Commissioner's Office.

Summary guidelines of records retention periods for schools

Please Note:

Due to the ongoing Independent Inquiry into Child Sexual Abuse (IICSA) no pupil and staff record should be destroyed until further notice. The guidance below gives a retention period (in the 'Retention Action' column), but where records should **not be** destroyed, this has been noted in the 'Disposal Action' column.

Introduction

These guidelines have been produced by ACET to assist schools in the management of their records. The guidelines outline the recommended retention periods for schools based on legislation and common practice.

It is the responsibility of Academies to retain their records for the appropriate retention period, or to transfer their historical records (those specifically highlighted in this document) to ACET Record Department. The retention guidelines produced in this document are some of the key retention periods which need to be considered. For a comprehensive list of retention periods schools should consult the Schools Toolkit produced by the Information and Records Management Society available at https://irms.org.uk/page/SchoolsToolkit

Explanatory Notes

The retention guidelines will outline a description of records, followed by the action to be taken in (e.g. retain for 3 years). This will be based on an event/action which will trigger that retention action (e.g. date record created). The disposal action will either be the destruction of the records, or their transfer to the ACET Record Department.

These guidelines may include references to records which are no longer routinely created as part of school business (e.g. log books). These have been included to assist schools who have a large backlog of historical records which require reviewing.

Under the Freedom of Information Act 2000. LA schools (including schools which are granted academy status) are regarded as public bodies and are subject to the Act. This requires that schools manage their records appropriately against agreed retention periods.

Glossary of Terms:

Business decision: if there is no law or regulation to say how long a record should be kept, we may base this decision on the administrative needs of ACET.

Closure: when a record ceases to be 'current' – this can be the when a set of minutes are formally agreed, or when a Help Desk incident is formally closed. Many retention periods are triggered after the 'closure' of a record.

Common practice: if there is no law or regulation to say how long a record should be kept, we may base this decision on what similar organisations do.

Disposal: the processes associated with the end of a records lifecycle, they will typically include destruction of the records or transfer of the records to ACET Record Office for permanent preservation

Functional Description: the description of the function that the record serves (i.e. the functional description of a set of minutes is 'the process of preparing business…')

Permanent: Retain the record permanently and offer to ACET Record Office

Record: the recorded evidence about an activity

Retention Action: the action regarding the retention of a record, triggered by a particular event (e.g. closure of a record)

For further information about the contents of this retention schedule, or for records management generally contact the Data Controller at datacontroller@astoncetrust.org

Ref. No.	Functional Description	Retention Period	Trigger	Disposal action	Basis for retention	Comments
CHILD PROTECTION						
SCH 1.1	Child protection files (primary school)	Retain for the duration of the pupil's attendance at the school	Date pupil changes school	Transfer to Secondary School	Keeping Children Safe in Education (Department for Education)	Where a child is removed from the roll to be educated at home/missing from education see below
SCH 1.2	Child protection files (secondary school)	Retain for 25 years	Pupil's date of birth	**Do not** destroy (refer to note on front page) Consider transfer to off-site storage on child reaching school leaving age	"Safeguarding Children in Education" 2004 Keeping Children Safe in Education (Department for Education)	Where a child is removed from the roll to be educated at home/missing from education see below
SCH 1.3	Child protection files (Child missing from education, Traveler, Roma, and therefore removed from roll)	Retain for 25 years (as above)	Date removed from roll	Transfer to ACET Record Office	"Safeguarding Children in Education" 2004 Keeping Children Safe in Education (Department for Education)	Scan all your documents into one folder and send via the Secure Portal

Ref. No.	Functional Description	Retention Period	Trigger	Disposal action	Basis for retention	Comments
SCH 1.4	Child protection files (child is removed from the roll and is Elective Home Educated)	Retain for 25 years (as above)	Date removed from roll	Transfer to ACET Record Office	"Safeguarding Children in Education" 2004 Keeping Children Safe in Education (Department for Education)	Scan all your documents into one folder and send via the Secure Portal
SCH 1.5	Allegations of a child protection nature made against a member of staff (including unfounded allegations)	Retain until the normal retirement age for the member of staff or for 10 years (whichever is the longer)	Employee's retirement age	**Do not** destroy (refer to note on front page)	Employment Practices Code: Supplementary Guidance (Information Commissioner's Office)	
GOVERNORS						
SCH 2.1	Principal set of signed minutes	Retain at school for 6 years	Date of meeting	Transfer to ACET Record Office	Common practice	
SCH 2.2	Inspection copies of minutes	Retain for 3 years	Date of Meeting	Destroy	Common practice	
SCH 2.3	Agendas	No retention required	Conclusion of meeting	Destroy	Common practice	

Ref. No.	Functional Description	Retention Period	Trigger	Disposal action	Basis for retention	Comments
SCH 2.4	Reports	Retain at school for 6 years	Date of report	Transfer to ACET Record Office	Common practice	
SCH 2.5	Annual parents meeting papers	Retain at school for 6 years	Date of meeting	Transfer to ACET Record Office	Common practice	
SCH 2.6	Instrument of Government	Retain at school for the duration of its operation	Closure of school	Transfer to ACET Record Office	Common practice	
SCH 2.7	Trusts and Endowments	Retain at school whilst operationally required	End of operational use	Transfer to ACET Record Office	Common practice	
SCH 2.8	Action Plans	Retain for 3 years	Expiration of action plan	Destroy	Common practice	May be appropriate to offer to ACET Record Department
SCH 2.9	Policy documents	Retain while policy is used operationally	Expiration of policy	Transfer to archives when policy is no longer operational	Common practice	
SCH 2.10	Complaints files	Retain for 6 years	Resolution of complaint	Review and destroy if complaints are non-contentious	Common practice	

Ref. No.	Functional Description	Retention Period	Trigger	Disposal action	Basis for retention	Comments
SCH 2.11	Annual reports required by central government	Retain at school for 10 years	End of the calendar year that the record was created in	Transfer to ACET Record Office	Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002	
SCHOOL MANAGEMENT						
SCH 3.1	Log books	Retain at school for 6 years	Date of last entry in log book	Transfer to ACET Record Office	Common practice	Legislation no longer requires the completion of a school log book
SCH 3.2	Minutes of management team	Retain at school for 5 years	Date of meeting	Transfer to ACET Record Office	Common practice	
SCH 3.3	Reports made by management team	Retain at school for 3 years	Date of report	Transfer to ACET Record Office	Common practice	
SCH 3.4	Development plans	Retain for 6 years	Expiry of plan	Review with a view to destroy	Common practice	May be appropriate offer to ACET Record Office
SCH 3.5	Successful school admissions applications	Retain for 1 year	Date of admission	Destroy	Common practice	
SCH 3.6	Unsuccessful school admission applications (where no appeal is made)	Retain for 1 year	Start of school term	Destroy	School Admissions Appeals Code 2012	

Ref. No.	Functional Description	Retention Period	Trigger	Disposal action	Basis for retention	Comments
SCH 3.7	Unsuccessful school admission applications (where an appeal is made)	Retain for 1 year	Resolution of case	Destroy	School Admissions Appeals Code 2012	
SCH 3.8	Proofs of address supplied by parents as part of the admissions process	Retain for 1 year	Date of admission	Destroy	Common practice	
PUPIL RECORDS						
SCH 4.1	Admission registers	Retain for 6 years	Last entry in register	Transfer to ACET Record Office	Common practice	These are no longer created in paper format
SCH 4.2	Attendance registers	Retain for 3 years	Last entry in register	Destroy	Common practice	
SCH 4.3	Pupil files (primary school)	Retain for duration of the pupil's attendance at school	Date pupil changes school	Transfer to Secondary School	Common practice	In the case of school exclusions it may be appropriate to transfer to ACET Record Office
SCH 4.4	Pupil files (secondary school school)	Retain for 25 years	Pupil's date of birth	**Do not** destroy (refer to note on front page)	The Limitations Act 1980	
SCH 4.5	Special educational needs records relating to individual support provided by the schools (primary)	Retain for duration of attendance at school	Date pupil changes school	Transfer to Secondary School	Common practice	

Ref. No.	Functional Description	Retention Period	Trigger	Disposal action	Basis for retention	Comments
SCH 4.6	Special educational needs records relating to individual support provided by the schools (secondary)	Retain for 35 years	Pupil's date of birth	**Do not** destroy (refer to note on front page)	Special Educational Needs and Disability Act 2001	This period is recommended by Derbyshire County Council.
SCH 4.7	Letters authorising absence	Retain for 2 years	Date of absence	Destroy	Common practice	
SCH 4.8	Public examination results	Retain for 6 years	Date of examination	Destroy	Common practice	
SCH 4.9	Internal school examination result	Retain for 5 years	Date of examination	Destroy	Common practice	
SCH 4.10	Advice and information issued by the school to parents regarding educational needs for individual pupils	Retain for 12 years	Date advice issued	Destroy	Special Educational Needs and Disability Act 2001	
SCH 4.11	Accessibility Strategy	Retain for 12 years	Expiry of strategy	Destroy	Special Educational Needs and Disability Act 2001	May be appropriate to offer to ACET Record Office
SCH 4.12	Parental permission slips for school trips where there has not been a major incident	No retention required	Conclusion of trip	Destroy	Common practice	
SCH 4.13	Parental permission slips for school trips **where there has been a major incident**	Retain for 25 years from the date of birth of the pupil/s involved in the incident	Pupil's date of birth	Destroy	The Limitations Act 1980	

Ref. No.	Functional Description	Retention Period	Trigger	Disposal action	Basis for retention	Comments
SCH 4.14	Records created by schools to obtain approval to run an Educational Visit outside the classroom where there has not been a major incident	Retain for 14 years	Date of visit	Destroy	The Health and Safety at Work Act 1974	Records created might include risk assessments
SCH 4.15	Records created by schools to obtain approval to run an Educational Visit outside the classroom **where there has been a major incident**	Retain for 21 years from the date of birth of the pupil/s involved in the incident	Pupil's date of birth	Destroy	The Limitations Act 1980	Records created might include risk assessments
SCH 4.16	Walking bus register	Retain for 3 years	Last entry in register	Destroy	Common practice	If there has been an incident it is assumed that an accident report will have been made and should be retained for the appropriate retention period (see Health and Safety section below)

Ref. No.	Functional Description	Retention Period	Trigger	Disposal action	Basis for retention	Comments
CURRICULUM						
SCH 5.1	Curriculum development	Retain for 6 years	End of the calendar year that the record was created in	Destroy	Common practice	
SCH 5.2	Curriculum returns	Retain for 3 years	End of the calendar year that the record was created in	Destroy	Common practice	
SCH 5.3	School syllabus	Retain for 1 year	Expiration of syllabus	Destroy	Common practice	May be appropriate to offer to ACET Record Office
SCH 5.4	Schemes of work	Retain for 1 year	End of the calendar year that the record was created in	Review with a view to destroy	Common practice	
SCH 5.5	Timetable development	Retain for 1 year	End of the calendar	Review with a view to destroy	Common practice	

Ref. No.	Functional Description	Retention Period	Trigger	Disposal action	Basis for retention	Comments
			year that the record was created in			
SCH 5.6	Records of marks awarded	Retain for 1 year	End of the calendar year that the record was created in	Destroy	Common practice	
SCH 5.7	Records of homework set	Retain for 1 year	End of the calendar year that the record was created in	Destroy	Common practice	
PERSONNEL						
SCH 6.1	Staff personnel files	Retain for 7 years	End of employment	**Do not** destroy (refer to note on front page)	Common practice	
SCH 6.2	Interview notes for successful candidates	Retain and add to personnel file.			Common practice	
SCH 6.3	Interview notes for unsuccessful candidates	Retain for 6 months	Date successful candidate is in post	Destroy	Common practice	

Ref. No.	Functional Description	Retention Period	Trigger	Disposal action	Basis for retention	Comments
SCH 6.4	Pre-employment vetting information (including DBS checks)	Retain for 6 months	Date information checked	Destroy	DBS guidelines	
SCH 6.5	Written warnings (level 1)	Retain for 6 months	Date of warning	**Do not** destroy (refer to note on front page)	Common practice	
SCH 6.6	Written warning (level 2)	Retain for 12 months	Date of warning	**Do not** destroy (refer to note on front page)	Common practice	
SCH 6.7	Final warning	Retain for 18 months	Date of warning	**Do not** destroy (refer to note on front page)	Common practice	
SCH 6.8	Warnings subsequently found to be based on an unfounded case (excluding child protection related warning)	No retention required	Date case found to be unfounded	**Do not** destroy (refer to note on front page)	Common practice	For child protection related warnings see Child Protection section above.
SCH 6.9	Staff appraisal records	Retain for 5 years	End of the calendar year that the record was created in	**Do not** destroy (refer to note on front page)	Common practice	
HEALTH AND SAFETY						
SCH 7.1	Accessibility Plans	Retain for 6 years	End of the calendar	Destroy	Disability and Equality Act 2010	

Ref. No.	Functional Description	Retention Period	Trigger	Disposal action	Basis for retention	Comments
			year that the record was created in			
SCH 7.2	Accident/incident reporting (adults)	Retain for 7 years	Date of incident	Destroy	Common practice	
SCH 7.3	Accident/incident reporting (children)	Retain for 25 years	Child's date of birth	Destroy	The Limitations Act 1980	
SCH 7.4	Records of monitoring areas where employees/pupils are likely to come into contact with asbestos	Retain for 40 years	Last action on file	Destroy	The Control of Substances Hazardous to Health Regulations 2002	
SCH 7.5	Records of monitoring areas where employees/pupils are likely to come into contact with radiation	Retain for 50 years	Last action on file	Destroy	The Ionising Radiations Regulations 1985	
SCH 7.6	Fire log books	Retain for 7 years	End of calendar year	Destroy	Common practice	
SCH 7.7	Records of the administration of medicines for all routine medication (e.g. Calpol, antibiotics, treatments for asthma and diabetes)	Retain for 1 year	End of calendar year	Destroy	Business decision	Events significantly outside individual treatment plan should be treated as non-routine (see below)

Ref. No.	Functional Description	Retention Period	Trigger	Disposal action	Basis for retention	Comments
SCH 7.8	Records of administration of medicines for all non-routine medication (e.g. peg feeding, epi-pen, invasive drugs, anti-depressants) and any records governing a reported incident, difficulty or issues with administering medication.	Retain for 21 years and 6 months from pupil's date of birth	Pupil's date of birth	Destroy	Business decision	
ADMINISTRATION						
SCH 8.1	Employer's Liability Certificate	Retain for 40 years	Closure of school		Common practice	Transfer to ACET Record Office on closure of school
SCH 8.2	Inventories of equipment/furniture	Retain for 6 years	End of calendar year	Destroy	Common practice	
SCH 8.3	Circulars to parents/staff/pupils	Retain for 1 year	End of calendar year	Destroy	Common practice	
SCH 8.4	Newsletters produced by the school	Retain for 1 year	End of calendar year	Transfer to ACET Record Office	Common practice	
SCH 8.5	Visitor books	Retain for 2 years	End of calendar year	Destroy	Common practice	

Ref. No.	Functional Description	Retention Period	Trigger	Disposal action	Basis for retention	Comments
FINANCE						
SCH 9.1	Annual accounts	Retain at school for 6 years	End of calendar year	Transfer to ACET Record Office	Common practice	
SCH 9.2	Invoices, receipts, and other financial records covered by financial regulations	Retain for 6 years	End of calendar year	Destroy	Standard financial regulations	
SCH 9.3	Annual budget and supporting papers	Retain for 6 years	End of calendar year	Destroy	Common practice	
SCH 9.4	Ordinary contracts	Retain for 6 years	End of contract	Destroy	The Limitations Act 1980	
SCH 9.5	Contracts under seal	Retain for 12 years	End of contract	Destroy	The Limitations Act 1980	
PROPERTY						
SCH 10.1	Building plans	Retain whilst operational	End of operational use	Transfer to ACET Record Office	Common practice	
SCH 10.2	Burglary, theft and vandalism report forms	Retain for 6 years	End of the calendar year that the record was created in	Destroy	Common practice	

Ref. No.	Functional Description	Retention Period	Trigger	Disposal action	Basis for retention	Comments
SCH 10.3	Contractors' reports	Retain for 6 years	End of the calendar year that the record was created in	Destroy	Common practice	
LOCAL AUTHORITY						
SCH 11.1	Secondary transfer sheets	Retain for 2 years	Year of transfer	Destroy	Common practice	
SCH 11.2	Attendance returns	Retain for 1 year	End of the calendar year that the record was created in	Destroy	Common practice	
CENTRAL GOVERNMENT						
SCH 12.1	Ofsted reports and papers	Retain whilst current	Date new report issued	Transfer to ACET Record Office	Common practice	Replace old report with new report
SCH 12.2	Returns to central government	Retain for 6 years	End of the calendar year that the record was created in	Destroy	Common practice	

Appendix 3

A step by step guide for what to do in the event of a data breach

If you have just become aware of a data breach at your Academy you need to act quickly.

Please remember you only have 72 hours to notify the Information Commissioners Office of a reportable breach, so you need to take the following steps promptly in order to identify if your breach is reportable.

Managing a data breach

In the event that the school identifies or is notified of a personal data breach, the following steps should be followed:

1. The person who discovers/receives a report of a breach must inform the Associate Principal or, in their absence, a nominated representative (which should be a member of the SLT) and/or ACET's Data Protection Officer (DPO). If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.
2. The Associate Principal or DPO (or nominated representative) must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff such as the IT technician.
3. The Associate Principal or DPO (or nominated representative) must inform the Chair of Governors as soon as possible. As a registered Data Controller, it is ACET's responsibility to take the appropriate action and conduct any investigation.
4. The Associate Principal or DPO (or nominated representative) must also consider whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future. In such instances, advice from the Academy's legal support should be obtained.
5. The Associate Principal or DPO (or nominated representative) must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

- Attempting to recover lost equipment.
- Contacting the relevant Trust's relevant Departments, so that they are prepared for any potentially inappropriate enquiries ('phishing') for further information on the individual or individuals concerned. Consideration should be given to a global email to all school staff. If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer's name and contact details if possible and confirm that they will ring the individual, making the enquiry, back. Whatever the outcome of the call, it should be reported immediately to the Associate Principal or DPO (or nominated representative)
- The use of back-ups to restore lost/damaged/stolen data
- If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use
- If the data breach includes any entry codes or IT system passwords, then these must be changed immediately and the relevant agencies and members of staff informed

Types of breach

- Data protection breaches could be caused by a number of factors. A number of examples are shown:
- Loss or theft of pupil, staff or governing body data and/ or equipment on which data is stored.
- Inappropriate access controls allowing unauthorised use.
- Equipment failure.

- Poor data destruction procedures.
- Human error.
- Cyber-attack.
- Hacking

Notifying other people or agencies
Some people or agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an initial investigation has taken place. The Associate Principal or DPO (or nominated representative) should, after seeking expert or legal advice, decide whether anyone is notified of the breach. In the case of significant breaches, the Information Commissioner's Office (ICO) must be notified within 72 hours of the breach. Every incident should be considered on a case by case basis.

When notifying individuals, give specific and clear advice on what they can do to protect themselves and what the school is able to do to help them. You should also give them the opportunity to make a formal complaint if they wish. The notification should include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to mitigate the risks posed by the breach.

Review and evaluation
Once the initial aftermath of the breach is over, the Associate Principal or DPO (or nominated representative) should fully review both the causes of the breach and the effectiveness of the response to it. It should be reported to the next available Senior Management Team and Full Governors meeting for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right. If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with Human Resources for advice and guidance. This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

Implementation
The Associate Principal or DPO (or nominated representative) should ensure that staff are aware of the Academy's Data Protection policy and its requirements including this breach procedure. This should be undertaken as part of induction, supervision and ongoing training. If staff have any queries in relation to the Academy's Data Protection policy and associated procedures, they should discuss this with their line manager, DPO or the Associate Principal.

Contact us
If you have a query about GDPR please contact us by email: datacontroller@astoncetrust.org