



Data Protection Policy

Date approved:	June 2026
Date of next review:	June 2027

Context and overview

Achievement Through Collaboration Trust (AtC) needs to gather and use certain personal information about individuals. This can include learners, parents, staff and Governors.

All data must be collected, stored and managed in accordance with UK and EU law, and in line with our trust ethos and values. Individuals retain the rights over their own data at all times. Our use of their data must be fair and lawful, and we must be open and honest about what we do with people's data.

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 (DPA)
- School Standards and Framework Act 1998
- Freedom of Information Act 2000
- Electronic Commerce (EC Directive) Regulations 2002
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2018)
- Protection of Freedoms Act 2012
- This policy also has regard to the following guidance:
- ICO (2021) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- ICO (2012) 'IT asset disposal for organisations'
- DfE (2018) 'Data protection: a toolkit for schools'

The use of personal data is governed by EU and UK law. This is enhanced and explained by case law and best practice.

In order to comply with the law, personal data must be collected fairly and lawfully. It must be stored safely and managed securely. It must not be disclosed to anyone who does not have authority to see it.

The General Data Protection Regulations (GDPR) (EU) 2016/679 set out how data should be obtained, stored and handled. These regulations set out six principles that underpin lawful use of data. These provide the foundation for good data governance. These principles are enhanced by a range of powers for individuals to control how their data is processed and stored.

Key principles

- Individuals retain rights over their data
- Data should be collected fairly and lawfully and used only in ways that the individual would expect
- Data should only be kept for as long as is necessary
- Data integrity and security is paramount
- Data governance will be actively managed at all levels of the organisation, to minimise risks to both the individual and the organisation
- All collection and use of data will be open and honest

Rationale

This policy will help ensure that AtC respects the rights of all individuals whose data it collects, including learners, parents, staff and Governors. It encompasses legal responsibilities and best practice. By being open and honest with individuals we will demonstrate that people can trust our organisation and that we handle personal data with integrity. Routine application of these principles will also help protect AtC from the risk of data breaches and unauthorised access to personal information.

Policy Scope

This policy applies to:

- All sites within our organisation
- Our teaching staff, support staff, Trustees and Governors
- Contractors, suppliers and anyone working on our behalf

Responsibilities under this policy

Everyone who works with or for AtC has some responsibility for ensuring that data is handled safely, securely and appropriately.

There are key roles within the organisation that carry specific responsibilities.

The Board of Trustees are the strategic lead body for the Trust. They will bear ultimate responsibility for ensuring that all our legal obligations are met. They will be accountable for any failure to abide by the correct regulations and for any impact that they may have on our learning community and our reputation within the local area.

The Chief Executive Officer (CEO) and individual school Senior Leadership Teams are the operational lead body for the Trust. They must ensure that all relevant policies and procedures are in place, and that practice follows the policy across all teams and trust areas. They will liaise with the Data Protection Officer in the event of any data governance issues that require attention, and will have overall responsibility for setting an appropriate tone of respect for personal data within the Trust.

The Data Protection Officer, or Data Protection Lead, has a key role to play in providing expert advice and guidance to the Board and the Senior Leadership Team. It is their responsibility to update senior management and the Board about Data Protection issues, and update policies and procedures in accordance with an agreed schedule and following legislative and best practice updates. They will oversee training and guidance for all staff, and be responsible for liaison with 3rd party suppliers, contractors and partners if they handle personal data. They will also oversee any Subject Access Requests, and handle the response to any data breaches, including being the point of contact for the public and notifying the ICO where necessary.

The TEL group act as Trust Network Manager and are responsible for ensuring the physical and virtual integrity of IT data storage services, systems and equipment. They will ensure all IT security meets acceptable professional standards, appropriate to the needs of the organisation, and that access to all electronic systems, databases or files is managed in accordance with the relevant policies. They will liaise with any 3rd party used for processing data, such as an HR / payroll supplier or cloud computing provider, to ensure appropriate levels of protection for all personal data. They have responsibility for making sure that customer-facing applications such as websites or online forms comply with relevant regulations including cookie policies and privacy notices. They will also oversee the life-cycle of data, software and hardware, ensuring that the processes for deleting or encrypting files in accordance with Retention Policies function effectively.

What is personal data?

Personal data is information about a person - anything that would allow someone to identify an individual. Processing that data means obtaining, using, and transferring data, and storing it in any system that allows it to be found again, such as a computer database or filing system.

For the purpose of this policy, 'personal data' refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g. an IP address. The UK GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

'Sensitive personal data' is referred to in the UK GDPR as 'special categories of personal data', and is defined as:

- Genetic data.

- Biometric data.
- Data concerning health.
- Data concerning a person's sex life.
- Data concerning a person's sexual orientation.
- Personal data which reveals:
 - Racial or ethnic origin.
 - Political opinions.
 - Religious or philosophical beliefs.
 - Trade union membership.

Principles.

'Sensitive personal data' does not include data about criminal allegations, proceedings or convictions. In the case of criminal offence data, schools are only able to process this if it is either:

- Under the control of official authority; or
- Authorised by domestic law.

The latter point can only be used if the conditions of the reason for storing and requiring the data fall into one of the conditions below:

The processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller of the data subject in connection with employment, social security, social protection, health or social care purposes, public health, and research.

In accordance with the requirements outlined in the UK GDPR, personal data will be:

Processed lawfully, fairly and in a transparent manner in relation to individuals.

Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered incompatible with the initial purposes.

Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals.

Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The UK GDPR also requires that “the controller shall be responsible for, and able to demonstrate, compliance with” the above principles.

Our Privacy Notice

AtC will take all reasonable steps to ensure that individuals are aware their data is being processed. This will include telling individuals what is being used, how it is being used, how long it will be kept for, and how they can exercise their rights in respect of that data.

Our Privacy Notice sets out how we collect data, what data we collect, the lawful basis for that, and how long we retain it. It includes information on who we share data with and the lawful basis for such sharing. It also sets out how people can request copies of data we hold about them. The Notice will be included in any marketing or information literature the company produces. It will also be available on request, and on the organisation's website.

Keeping personal data secure

Once personal data has been lawfully and fairly collected and processed, it must be safely stored, kept up to date, and safely accessed. Storing data in a way that complies with the regulations is a mix of common sense, clear processes and application of strong IT solutions.

The only people who will have access to personal data at AtC are those who need it for their work. Our IT systems and file storage will have granular levels of permission, and we will ensure that people only see personal data if required for operational reasons and for the benefit of teaching and learning.

Strong passwords must be used to access electronic resources and IT systems. These should never be shared with other people, or written down. AtC will set an appropriate password policy and require passwords to be changed on a regular basis.

Personal data must only be disclosed to those who are authorised to see it, both within and outside the organisation. If there is any doubt about the identity of the person requesting access to information, or doubt as to whether they should be allowed to see it, do not disclose information.

Data will only be shared with those people who are authorised to see it. This will be in line with our legal obligations and with the lawful and legitimate requirements of the business. Our Privacy Notice explains who we might share data with, the lawful basis for that, and the circumstances in which you can object to data being shared.

Training will be available for all staff. This will help them understand their responsibilities under data protection legislation. Staff should ask their line manager or the Data Protection Officer for guidance if they are unsure about any aspect of data protection.

Data use and transfer

Data must only be used for the purpose it was first obtained. Personal data should not be shared informally, either internally or externally to the organisation.

Staff should follow simple checks when transferring data outside the organisation via post or email, to ensure that personal data goes to the correct recipient. AtC will use a simple checklist (see appendix A) when sending personal data by post, to add an extra layer of security and checking to our data transfers.

Extra care must be taken when sharing data via email. This might include encryption or use of a secure email client.

Data should not be stored on personal IT devices. In particular, staff must not email school documents to their personal email addresses. If data needs to be transferred outside of the secure school environment, staff should use their school email account or a secure cloud storage solution provided by the ICT department.

Marketing and Promotion

AtC does carry out marketing and promotion.

When requesting school visits or brochures, or signing up for more information at Open Days, prospective parents will be informed how their data will be stored and how often we might contact them, and given the opportunity to decline to be contacted in the future.

We will ensure that anyone receiving marketing or promotion communications from us has given positive consent to receiving those communications, in the format that we send them out.

All our marketing and promotion communications will include a simple process for being removed from future communications.

CCTV

AtC does use CCTV cameras on our sites. This is to ensure the safety and security of those in our learning community, and to protect the site from damage. Our use of CCTV follows best practice guidelines as laid down by the ICO.

Images recorded by the CCTV cameras are stored on a separate server, in a secure location. They are retained for a maximum of 28 days, after which time they are securely overwritten.

Access to the images is restricted to specific people within the individual schools. We will only view CCTV footage in response to an incident or an allegation.

The images on our CCTV system are of a sufficient quality to allow us to make out faces of individuals in most circumstances. We are able to take copies of relevant parts of the CCTV footage and store it securely, in order to assist investigations into incidents or allegations.

In certain circumstances we may share CCTV footage with partners or other agencies. This may include senior leaders, parents, the Local Authority or the Police.

You can ask to see CCTV footage in which your image is captured. This should be done in writing as part of a Subject Access Request.

Getting your consent to process your personal data

There may be times when we would like to process your data in a way that requires your consent. This could include taking photographs, images or recordings of you engaging in school activities, or adding your contact details to any marketing or promotional mailing lists. It would also include getting your agreement to take and use finger or thumbprint information, to be used to access our catering payment services.

The Trust will ensure that we obtain your consent in a positive and clear way. You will be able to refuse consent, and that will not impact your ability to join in the full range of activities and opportunities within the Trust. If you do not wish to use thumb or fingerprint recognition, we will provide an easy alternative. We will also ensure that you can withdraw consent quickly and easily, should you change your mind about us processing your data in these ways.

Subject Access Requests

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

AtC will verify the identity of the person making the request before any information is supplied.

A copy of the information will be supplied to the individual free of charge; however, AtC may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual requests further copies of the same information. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged. All fees will be based on the administrative cost of providing the information.

Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

Where a SAR has been made for information held about a child, AtC will evaluate whether the child is capable of fully understanding their rights. If AtC determines the child can understand their rights, it will respond directly to the child.

All requests will be responded to without delay and at the latest, within one month of receipt. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

Where a request is manifestly unfounded or excessive, AtC holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

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

Omit certain elements from the response if another individual's personal data would be disclosed otherwise.

Reject requests that cannot be fulfilled without disclosing another individual's personal data, unless that individual consents or it is reasonable to comply without consent.

Explain to the individual who made the SAR why their request could not be responded to in full.

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

The right to rectification

Individuals, including children, are entitled to have any inaccurate or incomplete personal data rectified.

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

Requests for rectification will be investigated and resolved, where appropriate, free of charge; however, AtC may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual makes multiple requests at once. AtC reserves the right to refuse to process requests for rectification if they are manifestly unfounded or excessive or if exemptions apply.

AtC will take reasonable steps to ensure that data is accurate or is rectified if inaccurate, implementing a proportional response for data that has a significant impact on the individual, e.g. if significant decisions are made using that data. We will restrict processing of the data in question whilst its accuracy is being verified, where possible.

Where the personal data in question has been disclosed to third parties, AtC will inform them of the rectification where possible. Where appropriate, AtC will inform the individual about the third parties that the data has been disclosed to.

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

The right to erasure

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

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

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

- AtC has the right to refuse a request for erasure where the personal data is being processed for the following reasons:
- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority

- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The establishment, exercise or defence of legal claims

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

Public health purposes in the public interest, e.g. protecting against serious cross-border threats to health.

Purposes of preventative or occupational medicine, the working capacity of an employee, medical diagnosis, the provision of health or social care, or the management of health or social care systems or services.

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

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

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

The right to restrict processing

Individuals, including children, have the right to block or suppress AtC's processing of personal data.

AtC 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 AtC has verified the accuracy of the data

Where an individual has objected to the processing and AtC 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 AtC no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

In the event that processing is restricted, AtC 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. AtC will inform individuals when a restriction on processing has been lifted.

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

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

AtC reserves the right to refuse requests for restricting processing if they are manifestly unfounded or excessive or if exemptions apply. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

The right to data portability

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

Where personal data has been provided directly by an individual to a controller

Where the processing is based on the individual's consent or for the performance of a contract

When processing is carried out by automated means

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

AtC will provide the information free of charge.

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

AtC will respond to any requests for portability within one month. Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

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

The right to object

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

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

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

An individual's grounds for objecting must relate to his or her particular situation.

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

AtC will respond to objections proportionally, granting more weight to an individual's objection if the processing of their data is causing them substantial damage or distress.

Where personal data is processed for direct marketing purposes:

- The right to object is absolute and AtC will stop processing personal data for direct marketing purposes as soon as an objection is received.
- We will not refuse an individual's objection regarding data that is being processed for direct marketing purposes.
- AtC will retain only enough information about the individual to ensure that the individual's preference not to receive direct marketing is respected in future.

Where personal data is processed for research purposes:

The individual must have grounds relating to their particular situation in order to exercise their right to object.

Where the processing of personal data is necessary for the performance of a public interest task, AtC is not required to comply with an objection to the processing of the data.

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

The DPO will ensure that details are recorded for all objections received, including those made by telephone or in person, and will clarify each objection with the individual making the request to avoid later disputes or misunderstandings. AtC will respond to all objections without undue delay and within one month of receiving the objection; this may be extended by a further two months if the request is complex or repetitive.

Where no action is being taken in response to an objection, AtC will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

Automated decision making and profiling

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

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

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

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

AtC will conduct a DPIA for automated decision making to mitigate risk of errors, bias and discrimination.

AtC will ensure that individuals concerned are given specific information about the processing and an opportunity to challenge or request a review of the decision.

Individuals have the right not to be subject to a decision when both of the following conditions are met:

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

AtC will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

When automatically processing personal data for profiling purposes, AtC will ensure that the appropriate safeguards are in place, including:

Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.

Using appropriate mathematical or statistical procedures.

Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.

Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

Data protection by design and default

AtC will act in accordance with the UK GDPR by adopting a data protection by design and default approach and implementing technical and organisational measures which demonstrate how AtC has considered and integrated data protection into all aspects of processing activities. In line with the data protection by default approach, AtC will ensure that only data that is necessary to achieve its specific purpose will be processed.

AtC will implement a data protection by design and default approach by using a number of methods, including, but not limited to:

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

Data Protection Impact Assessments (DPIAs)

DPIAs will be used in certain circumstances to identify the most effective method of complying with AtC's data protection obligations and meeting individuals' expectations of privacy. DPIAs will allow AtC to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to AtC's reputation which might otherwise occur. A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals, and will be used for more than one project, where necessary.

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

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

AtC will ensure that all DPIAs include the following information:

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

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

Data breaches

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The headteacher will ensure that all staff are made aware of, and understand, what constitutes a data breach as part of their training.

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

Where AtC faces a data security incident, the DPO will coordinate an effort to establish whether a personal data breach has occurred, assess the significance of any breach, and take prompt and appropriate steps to address it.

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

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed, and the individuals concerned will be contacted directly. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority. The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis. In the event that a breach is sufficiently serious, the public will be notified without undue delay.

Within a breach notification to the supervisory authority, the following information will be outlined:

The nature of the personal data breach, including the categories and approximate number of individuals and records concerned

The name and contact details of the DPO

An explanation of the likely consequences of the personal data breach

A description of the proposed measures to be taken to deal with the personal data breach

Where appropriate, a description of the measures taken to mitigate any possible adverse effects

Where notifying an individual about a breach to their personal data, AtC will provide specific and clear advice to individuals on the steps they can take to protect themselves and their data, where possible and appropriate to do so.

AtC will ensure all facts regarding the breach, the effects of the breach and any decision-making processes and actions taken are documented in line with the UK GDPR accountability principle and in accordance with the Records Management Policy.

AtC will work to identify the cause of the breach and assess how a recurrence can be prevented, e.g. by mandating data protection refresher training where the breach was a result of human error.

Safeguarding

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

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

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

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

Publication of information

The Trust (and its schools) publish a Freedom of Information Publication Scheme on its website outlining classes of information that will be made routinely available, including:

- Policies and procedures.
- Minutes of meetings.
- Annual reports.
- Financial information.
- Classes of information specified in the Freedom of Information Publication Scheme are made available quickly and easily on request.

Appendix A Confidential Post – Checklist

Sending out personal data by post is a potential source of data breaches. Information sent to the wrong address, or sent out without the contents being thoroughly checked, could allow personal data to be seen by people who have no reason to see it, or who should not be seeing it. Please use this form to ensure that you have carefully checked the contents, address details, and envelope.

Once completed, this form should be kept in a secure file, to be checked in the event of a postal data breach being discovered. Forms should be kept for a period of 3 months.

STATEMENT	TICK TO CONFIRM
There is a covering letter explaining the contents of the letter, and this is addressed to the correct person.	
Any additional content has been checked to ensure that it is the correct information to send to the named person.	
The address of the recipient is clearly visible through the envelope address window, or clearly written on the envelope.	
The envelope is marked 'Confidential; Addressee Only'.	
There is a return address clearly written or stamped on the envelope, in case the letter is not correctly delivered.	
If you are expecting data to be returned, you have included a stamped, addressed envelope, with sufficient postage, marked 'confidential'.	
The envelope is securely sealed.	

Recipient Name	
Name of person checking the letter	

Signed	
Date	