THE CONSORTIUM
ACADEMY TRUST

Shaping Positive Futures

Data Protection Policy

The Consortium Academy Trust (TCAT)
An Exempt Charity Limited by Guarantee
Company Number 07665828

Status:	Live
Policy Owner (position)	CEO / DPO
Statutory / Recommended	Statutory
Date Adopted	May 2018
Review Period	24 months
Last Review Date	January 2024
Revision	4
Next Review Date	January 2026
Advisory Committee	Trust Board
Linked Documents and Policies	ICT Acceptable Use Policy CCTV Policy, Protection of Biometric Data Records Management Policy and Freedom of Information Policy

**NB – This document can only be considered valid when viewed on The Consortium Academy Trust website. If the copy is printed or downloaded and saved elsewhere the Policy date should be cross referenced to ensure the current document is the latest version. The linked policies can be found at www.consortiumtrust.co.uk*

Contents:

Statement of Intent

The Consortium Academy Trust ("the Trust") in the course of its activities is required to keep and process certain information about its staff members, governors, learners and their families, suppliers and external contractors in accordance with its legal obligations under data protection legislation.

In this policy, the phrase "DP Legislation" shall mean the UK General Data Protection Regulation ((EU) 2016/679), the Data Protection Act 2018 and all other data protection legislation having effect in the United Kingdom.

DP Legislation imposes certain obligations on the Trust regarding the handling of personal data irrespective of whether such information is held on paper, on a computer or on other media.

This policy applies to every employee, governor, trustee, member, worker (including any agency, casual or temporary worker), volunteer and contractor who is employed or otherwise engaged at any academy operated by the Trust (each a "Data User").

The Trust may, from time to time, be required to share personal information about its staff or learners with other organisations, mainly the LA, DfE, other schools and educational bodies, and potentially children's services.
This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the Trust complies with the following core principles of the UK GDPR.

Organisational methods for keeping data secure are imperative, and the Trust believes that it is good practice to keep clear practical policies, backed up by written procedures. The Trust has prepared this policy in order to inform you of your obligations under DP Legislation and as a Data User in respect of the obtaining, handling, processing, storage, transportation and destruction of personal data. Each of these activities constitutes "processing" of personal data under DP Legislation. This policy informs you of our rules and procedures for processing personal data.

This policy should be read in conjunction with the following related Trust policies:

- ICT Acceptable Use Policy
- CCTV Policy
- Records Management Policy
- Freedom of Information Policy
- Protection of Biometric Data

1 Legal framework

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

- UK General Data Protection Regulation
- Data Protection Act 2018

- The Freedom of Information Act 2000
- Electronic Commerce (EC Directive) Regulations 2002
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2018)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998
- Protection of Freedoms Act 2012

This policy also has regard to the following guidance:

- ICO (2018) 'Guide to the General Data Protection Regulation (GDPR)'
- ICO (2012) 'IT asset disposal for organisations'
- DfE (2018) 'Data protection: a toolkit for schools'

2 Applicable data

For the purpose of this policy, **personal data** refers to information that relates to a living individual who can be identified (directly or indirectly) from that information alone or in combination with other identifiers in the Trust's possession or which the Trust can reasonably access. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that individual's actions or behaviour. It also includes online identifiers (e.g. an IP address).

DP Legislation 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 DP Legislation as 'special categories of personal data', which are broadly the same as those in the Data Protection Act 2018. These specifically include the processing of genetic data, biometric data, and data concerning health matters, political opinions, religious or philosophical beliefs, trade union membership, sex life and sexual orientation. The processing of such data is prohibited unless certain conditions are met.

3 Principles

In accordance with the requirements outlined in DP Legislation, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals (also known as "**data subjects**")
- 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 to be incompatible with the initial purposes. This means that personal data must not be collected for one purpose and used for another. If it becomes necessary to change the purpose for which personal data is processed, the data subject must be informed of the new purpose before such processing occurs

- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Any personal data which is not necessary for that purpose should not be collected
- 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. This means that personal data should be destroyed or erased from the Trust's systems when it is no longer required
- 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

DP Legislation also requires:

- The Trust to be responsible for, and able to demonstrate, compliance with the above principles. The Trust will be able to demonstrate how data is processed as a whole across the MAT, and will ensure each individual school within the Trust is adhering to the same procedure and that this is being implemented and enforced in line with the wider Trust policies
- Personal data to be processed in accordance with the rights of the individual to whom the personal data relates
- Personal data not to be transferred outside the European Economic Area unless adequate safeguards have been put in place to allow its export

4 Accountability

The Trust has put in place appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the DP Legislation.

The Trust will provide comprehensive, clear and transparent privacy policies.

Additional internal records of the Trust's processing activities will be maintained and kept up-to-date in accordance with DP Legislation.

These internal records of processing activities include the following:

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

The Trust will also document other aspects of compliance with the UK GDPR and DPA where this is deemed appropriate in certain circumstances by the DPO, including:

- Information required for privacy notices, e.g. the lawful basis for the processing
- Records of consent
- Controller-processor contracts
- The location of personal data
- Data Protection Impact Assessment (DPIA) reports
- Records of personal data breaches

The Trust will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Data minimisation
- Pseudonymisation
- Transparency
- Allowing individuals to monitor processing
- Continuously creating and improving security features

Data protection impact assessments will be used, where appropriate.

5 Data Protection Officer (DPO) and Data Protection Links

The Trust is required under DP Legislation to appoint a DPO, who will:

- Inform and advise the Trust and Data Users about their obligations to comply with the DP Legislation
- Monitor the Trust's compliance with the DP Legislation, including managing internal data protection activities, advising on data protection impact assessments, internal audits, and arranging for Data Users to receive any required training.
- Cooperate with the ICO and act as first point of contact for the ICO and for individuals whose data is being processed

The DPO for the Trust is Gilly Stafford (Compliance and Data Protection Manager) who is based at the Trust's headquarters at Cottingham High School and whose email address is dpo@consortiumtrust.co.uk.

The DPO will operate independently and will not be dismissed or penalised for performing their duties. Sufficient resources and appropriate access will be provided to the DPO to enable them to meet their UK GDPR obligations.

The DPO is responsible for:

- **C**oordinating a proactive and preventative approach to data protection
- Calculating and evaluating the risks associated with data processing
- Having regard to the nature, scope, context, and purposes of all data processing

- Prioritising and focussing on more risky activities, e.g. where special category data is being processed
- Promoting a culture of privacy awareness throughout the Trust community
- Carrying out ad hoc reviews of data practices to ensure staff understand and are acting in accordance with relevant data protection laws

We have also designated a member of staff at each academy to be a Data Protection Link. The email addresses for the Links are as follows:

- Cottingham High School and Sixth Form College- email dplink@cottinghamhigh.net
- Croxby Primary School -email dplink@croxbyprimary.co.uk
- Hessle Academy (including Hessle High School and Penshurst Primary School) - email dplink@hessleacademy.com
- Holderness Academy and Sixth Form College -email dplink@holderness.academy
- Howden School -email dplink@howdenschool.net
- Keyingham Primary School dplink@keyinghamprimary.co.uk
- Winifred Holtby Academy – email dplink@winifredholtbyacademy.com
- Wolfreton School and Sixth Form College– email dplink@wolfreton.co.uk

Any queries in relation to this policy or the handling of personal data within the Trust should be referred to the relevant school's Data Protection Link in the first instance, who may refer such queries to the DPO if the circumstances so require. Where appropriate, you will receive additional training in respect of the Trust's personal data handling and security procedures.

If you consider that this policy has not been followed in respect of personal data about yourself or others, you should raise the matter with the DPO.

6 Lawful processing

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

The Trust has privacy notices for the following groups, which outline the information above that is specific to them:

- Learners and their families
- Student (Year 7-11)
- Sixth Form learners
- Governors and Trustees
- Staff, volunteer, contractor and applicant

There may be circumstances where it is considered necessary to process personal data or special category personal data in order to protect the vital interests of a data subject. This may include medical emergencies where it is not possible for the data subject to give consent to the processing. In such circumstances, the DPO will be consulted and a decision made only after seeking further clarification.

Under the DP Legislation, at least one of the following conditions must apply in order for personal data to be lawfully processed:

- The consent of the data subject has been obtained; or
- The processing is necessary for:
  - Compliance with a legal obligation
  - The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
  - For the performance of a contract with the data subject or to take steps to enter into a contract
  - Protecting the vital interests of a data subject or another person
  - For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (This condition is not available to processing undertaken by the Trust in the performance of its public tasks)

In addition, sensitive personal data must only be processed if an additional processing condition specifically permitting the processing of sensitive personal data applies. Of these conditions, the ones of most likely potential relevance to the Trust are:

- The explicit consent of the data subject has been provided
- The processing relates to personal data manifestly made public by the data subject
- The processing is necessary for:
  - Carrying out obligations under employment, social security or social protection law, or a collective agreement
  - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
  - The establishment, exercise or defence of legal claims
  - Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards
  - The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional

7 Consent

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

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

Consent is sought from parents /carers for learners under 16. Learners 16 years and over can give their own consent.

Consent is sought for internal publicity (e.g. image on school noticeboards) external publicity (e.g. image on school / Trust website, transition booklets, social media accounts), biometric data, permission to leave site alone (for pupils in Years 3 to 6), medical consent (e.g. for vaccinations, emergency first aid, medicine), careers advice or to share data with third parties to raise aspirations.

Consents are collected via a parent portal /app and are live. The date of when consent is given (or withdrawn) is recorded in the portal /app.

The Trust has implemented procedures for ensuring that any consent mechanisms in operation meet the standards of the DP Legislation. Where such standard of consent cannot be met, an alternative valid legal basis for processing the data must be found, or the processing must cease.

Consent can be withdrawn at any time.

Where a child is under the age of 16, the consent of parents/carers will be checked prior to the processing of the child's data, except where the processing is related to preventative or counselling services offered directly to a child.

8 The right to be informed

Adults and children have the same right to be informed about how the Trust uses their data. The privacy notices supplied to individuals, including children, in regard to the processing of their personal data will be written in clear, plain, age-appropriate language which is concise, transparent, easily accessible and free of charge.

Each individual about whom we process personal data must be provided with a privacy notice which explains to them how the Trust will use their personal data. The Trust has put in place standard privacy notices for each category of individual about whom it ordinarily processes personal data (see 6.2).

The DP Legislation requires each such privacy notice to be written in clear, plain language which is concise, transparent, easily accessible and free of charge. All our privacy notices can be viewed at https://www.consortiumtrust.co.uk/statutory

The Trust has also put in a place a child-friendly privacy notice which is specifically addressed to students aged 11 and over and explains to them how the Trust will use their data in a clear, plain manner.

In relation to personal data (whether obtained directly from the data subject or indirectly via a third party), DP Legislation requires several pieces of information to be supplied as part of the relevant privacy notice, including but not limited to the following details:

- The identity and contact details of the controller (i.e. the Trust) and the DPO
- The purpose of, and the legal basis for, processing the data

- The legitimate interests of the controller or third party being relied upon (if applicable)
- Any recipient or categories of recipients of the personal data
- Details of any data transfers to third countries and the safeguards in place
- The applicable data retention period(s) or criteria used to determine those retention period(s)
- The existence of the data subject's rights, including the rights to:
  - Withdraw consent at any time
  - Lodge a complaint with a supervisory authority (e.g. the Information Commissioner's Office)

Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data

Where data is not obtained directly from the data subject, information regarding the categories of personal data that the Trust holds about them, the source that the personal data originates from and whether it came from publicly accessible sources

For personal data obtained directly from the data subject, this information must be supplied at the time the data is obtained.

In relation to personal data that is not obtained directly from the data subject, this information must be supplied within one month of having obtained the data or, if earlier:

- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
- If the data is used to communicate with the individual, at the latest, when the first communication takes place.

Where the Trust wishes to process personal data about any individual in a manner which has not previously been explained to them in the applicable privacy notice, the Trust will be required to explain such additional processing (and obtain any required consents) before carrying out such processing. This may be achieved by additional related wording on any subsequent information capture forms completed by the individual during their time with the relevant academy.

The Trust does not use automated decision-making processes.

The Trust does not use personal data for profiling purposes.

9 The right of access

Individuals (including children) have the right to obtain confirmation that their data is being processed.

Individuals have the right (subject to certain statutory exemptions) to submit a data subject access request ("DSAR") to gain access to their personal data.

If a parent / carer requests the data of their child and the child is 13 years or over, then we have to legally seek the consent of the child to release the data to their parent / carer

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

Subject to any applicable exemptions, a copy of the information will be supplied to the individual free of charge; however, the Trust may impose a 'reasonable fee' to comply with requests for further copies of the same information.

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

Where a request is manifestly unfounded, excessive or repetitive, either a reasonable fee will be charged or the Trust may refuse to provide the information. The individual must be informed of this decision and the reasoning behind it, as well as their right to complain to the ICO and to a judicial remedy, within one month of the refusal.

All fees will be based on the administrative cost of providing the information.

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

In the event that a large quantity of information is being processed about an individual, the Trust will ask the individual to specify the information the request is in relation to.

The school 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, the school 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.

Any Data User who receives a DSAR should forward it to the school Data Link DPO immediately (see section 5 above) and not respond directly to the request.

In addition, parents /carers have their own independent right under The Education (Pupil Information) (England) Regulations 2006 of access to the official education records of their children. Learners do not have the right to prevent their parents/carers from obtaining a copy of their school records.

10 The right to rectification

Individuals (including children) are entitled to have any inaccurate or incomplete personal data rectified. Any such request may be verbal or in writing.

Where the personal data in question has been disclosed to third parties, the Trust will inform them of the rectification where possible.

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

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

Where no action is being taken in response to a request for rectification, the Trust will explain the reason for this to the individual, and will inform them of their right to complain to the ICO and to a judicial remedy.

Any Data User who receives a rectification request should forward it to the school Data Link immediately (see section 5 above) and not respond directly to the request.

11 The right to erasure (also known as 'the right to be forgotten')

Individuals (including children) hold the right to request the deletion or removal of personal data in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation

The Trust has the right to refuse a request for erasure where the personal data is being processed for one of the following reasons:

- When the objection is in respect of the Trust's reliance on the legitimate interests condition but there exists an overriding legitimate interest for the Trust to continue the processing
- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes

- The exercise or defence of legal claims

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, the Trust will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

Any Data User who receives an erasure request should forward it to the school Data Link immediately (see section 5 above) and not respond directly to the request.

12 The right to restrict processing

Individuals (including children) have the right to block or suppress the Trust's processing of personal data in certain limited circumstances. In the event that processing is so restricted, the Trust may store certain 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.

The Trust will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the Trust has verified the accuracy of the data
- Where an individual has objected to the processing and the Trust is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restriction instead
- Where the Trust no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

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

The Trust will inform individuals when a restriction on processing has been lifted. Any Data User who receives a restriction request should forward it to the school Data Link immediately (see section 5 above) and not respond directly to the request.

13 The right to data portability

Individuals (including children) have the right to obtain and reuse their personal data for their own purposes from the Trust to another data controller in certain limited circumstances.

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

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

- To personal data that an individual has provided to a controller, **and**
- Where the processing is based on the individual's consent or for the performance of a contract**, and**
- When processing is carried out by automated means

Where the right to data portability is validly exercised, the relevant personal data will be provided to the other data controller in a structured, commonly used and machine-readable form.

The Trust will provide the information free of charge.

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

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

The Trust 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, the Trust 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 ICO and to a judicial remedy.

Any Data User who receives a request for portability should forward it to the school Data Link immediately (see section 5 above) and not respond directly to the request.

14 The right to object

The Trust 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 have the right to object to the following:

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

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

- An individual's grounds for objecting must relate to his or her particular situation
- The Trust will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the Trust can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the individual
- The Trust 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 the school will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The Trust cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.
- The Trust 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, the Trust is not required to comply with an objection to the processing of the data.

Any Data User who receives an objection request should forward it to the school Data Link immediately (see section 5 above) and not respond directly to the request.

15 Data protection by design and default

The Trust acts in accordance with the DP Legislation by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the Trust has considered and integrated data protection into processing activities.

Data protection impact assessments (DPIAs) will be used where required by the DP Legislation to identify the most effective method of complying with the Trust's data protection obligations and meeting individuals' expectations of privacy.

DPIAs will allow the Trust to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the Trust'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.

A DPIA 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.

The Trust has put in place procedures to 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, the Trust may consult the ICO to seek its opinion as to whether the processing operation complies with the DP Legislation.

Each DPIA will be overseen by the DPO.

16 Third party data processors

Where the Trust enters into an arrangement with a third party which involves the processing of personal data by one party on behalf of the other (e.g. under an outsourced services agreement or licence to use hosted software), the Trust will enter into a contract /data processing agreement with the third party which imposes certain minimum data security obligations on the party processing the data.
Each such arrangement must be reviewed by the DPO prior to commencement to ensure that all such clauses have been documented correctly.

Personal data may only be transferred to a third party processor if the processor agrees to comply with those procedures and policies, or puts in place adequate measures itself.

17 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. All staff will have training to be aware of, and understand, what constitutes a data breach.

Where the school faces a data security incident, the DP Link 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, consulting with the DPO when necessary

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

Where the school faces a data security incident, the DP Link 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 the school 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, the school /central 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.

We will ensure all facts regarding the breach will be documented in the data protection database.. We 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.

18 Data security

Confidential paper records will be kept in locked filing cabinets, drawers or a safe, with restricted access, and will not be left unattended or in clear view anywhere with general access.

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

Data Users should ensure that they lock or log off individual monitors /laptops when unattended.

Where appropriate, personal data should be anonymised.

Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted. All electronic devices are password-protected to protect the information on the device in case of theft. Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.

Where possible, staff and governors will not use their personal laptops or computers for school purposes. All members of staff are provided with their own secure login and password, and every computer prompts users to change their password according to the password policy.

Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient. Circular emails to parents/carers are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients. When sending confidential information staff will always check that the recipient is correct before sending. Personal comments and opinions in correspondence and other documents should be avoided wherever possible as individuals have the right to request copies of all the personal data that the Trust holds about them, including such written comments and opinions. All email messages may be disclosed in legal proceedings in the same way as paper documents and should be treated as potentially retrievable even after they have been deleted.

Before sharing data, all staff will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.

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

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

The physical security of the Trust's buildings and storage systems, and access to them, is reviewed periodically, but at least on a termly basis. If an increased risk in vandalism, burglary or theft is identified, extra measures to secure data storage will be put in place.

We will regularly test, assess and evaluate the effectiveness of any and all measures in place for data security.

The school takes its duties under the UK GDPR seriously and any unauthorised disclosure may result in disciplinary action. The Director of Information and Digital Transformation is responsible for continuity and recovery measures are in place to ensure the security of protected data.

When disposing of data, paper documents will be shredded / placed in secure waste bags. Digital storage devices will be physically destroyed when they are no longer required. ICT assets will be disposed of in accordance with the ICO's guidance on the disposal of ICT assets.

19 Disclosure and Barring Service ("DBS") data

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

Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

20 Safeguarding

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

We 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

We 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. The school will manage all instances of data sharing for the purposes of keeping a child safe in line with the Child Protection and Safeguarding Policy.

21 CCTV and Photography

The Trust understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles. We notify all learners, staff and visitors of the purpose for collecting CCTV images via notice boards and a privacy notice.

Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose. All CCTV footage will be kept for one month, longer for incidents pending investigations. We have a CCTV Policy on the Trust website. The Consortium Academy Trust - General Policies (consortiumtrust.co.uk)

Images captured by individuals for recreational or personal purposes, and videos made by parents for family use, are exempt from the UK GDPR.

Parents and others attending school events are able to take photographs and videos of those events as long as they are for domestic purposes only. Photographs or videos being used for any other purpose are prohibited to be taken by parents or visitors to the school.

The school asks that parents and others do not post any images or videos which include any children other than their own on any social media, or otherwise publish those images or videos.

22 Cloud computing

For the purposes of this policy, 'cloud computing' refers to storing and accessing data and programs, such as documents, photos or videos, over the internet, rather than on a device's hard drive. Cloud computing involves the Trust accessing a shared pool of ICT services remotely via a private network or the internet.

All staff will be made aware of data protection requirements and how these are impacted by the storing of data in the cloud, including that cloud usage does not prevent data subjects from exercising their data protection rights.

If the cloud service offers an authentication process, each user will have their own account. A system will be implemented to allow user accounts to be created, updated, suspended and deleted, and for credentials to be reset if they are forgotten, lost or stolen. Access for employees will be removed when they leave the school.

All files and personal data will be encrypted before they leave a school device and are placed in the cloud, including when the data is 'in transit' between the device and cloud. A robust encryption key management arrangement will be put in place to maintain protection of the encrypted data. The loss of an encryption key will be reported to the DPO immediately; failure to do so could result in accidental access or destruction of personal data and, therefore, a breach of the relevant data protection legislation.

As with files on school devices, only authorised parties will be able to access files on the cloud. An audit process will be put in place to alert the school should unauthorised access, deletion or modification occur, and ensure ongoing compliance with the school's policies for the use of cloud computing.

The school's usage of cloud computing, including the service's security and efficiency, will be assessed and monitored by the DPO. The DPO will also ensure that a contract and data processing agreement are in place with the service provider, confirming compliance with the principles of the UK GDPR and DPA. The agreement will specify the circumstances in which the service provider may access the personal data it processes, such as the provision of support services.

The DPO will also:

- Ensure that the service provider has completed a comprehensive and effective self-certification checklist covering data protection in the cloud.
- Ensure that the service provider can delete all copies of personal data within a timescale in line with the school's Data Protection Policy.

- Confirm that the service provider will remove all copies of data, including back-ups, if requested.
- Find out what will happen to personal data should the school decide to withdraw from the cloud service in the future.
- Assess the level of risk regarding network connectivity and make an informed decision as to whether the school is prepared to accept that risk.
- Monitor the use of the school's cloud service, with any suspicious or inappropriate behaviour of pupils, staff or parents being reported directly to the headteacher

23 Additional information

This policy does not form part of any employee's contract of employment and it may be amended by the Trust at any time.

If you are found to be in breach of the terms of this policy you may be subject to disciplinary proceedings which in serious cases, or in cases of repeated breach, may result in dismissal (and, in exceptional circumstances, criminal charges). If you are in any doubt about the terms of this policy or have any questions about this policy, please ask your relevant Data Protection Link for further guidance in the first instance (see section 5 above).

This policy will be reviewed at least every 2 years to ensure it is achieving its stated objectives.

THE CONSORTIUM
ACADEMY TRUST

Shaping Positive Futures

Data Protection Policy

I confirm that I have read and understood the contents of this Data Protection Policy

Signed…….

Print Name…….

Academy…….

Date…….

Please print this page, sign and hand in to your school Data Protection Link or for Governors please hand to your Governance Professional