THE CONSORTIUM
ACADEMY TRUST

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	N/A
Date Adopted	21 May 2018
Review Date	Annual
Advisory Committee	Trust Board
Linked Documents and Policies	ICT Acceptable Use Policy, CCTV Policy, Records Management Policy and Freedom of Information Policy

Contents:

Statement of Intent

The Consortium Academy Trust ("the Trust") in the course of its activities keeps and processes certain information about its staff members, governors, learners and their families, suppliers and other individuals.

In this policy, the phrase "**DP Legislation**" shall mean the 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 and you relating to how the Trust and you must handle 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**").

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 Safeguarding Policy
- CCTV Policy
- Records Management Policy
- Freedom of Information Policy

1. Legal framework

1.1. In addition to applicable DP Legislation, this policy has due regard to the following legislation:

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

1.2. This policy also has regard to the following guidance:

- ICO (2018) 'Guide to the General Data Protection Regulation (GDPR)'

2. Applicable data

2.1. 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).

2.2. 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.

2.3. **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 1998. 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

3.1. In accordance with the requirements outlined in the 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

3.2. DP Legislation also requires:

- The Trust to be responsible for, and able to demonstrate, compliance with the above principles
- 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

4.1. 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.

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

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

4.4. 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

4.5. 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

4.6. Data protection impact assessments will be used, where appropriate.

5. Data Protection Officer (DPO) and Data Protection Links

5.1. 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.

5.2. The DPO for the Trust is Gilly Stafford (Company Secretary/Clerk to the Trust), who is based at the Trust's headquarters at Cottingham High School and whose email address is dpo@consortiumtrust.co.uk.

5.3. We have also designated each of the following staff members as a Data Protection Link for the academies as listed below:

- Cottingham High School and Sixth Form college- Jo Tuffs (Data, Timetable and Information Systems Manager) – email dplink@cottinghamhigh.net
- Croxby Primary - Janette Truran (Senior Administrator and PA to SLT) - email dplink@croxbyprimary.co.uk
- Hessle Academy (including Hessle High and Penshurst Primary School) - Sarah Greenley (Operations Manager) - email dplink@hessleacademy.com
- Holderness Academy- Karen Mulkern (Systems and Information Manager) -email dplink@holderness.academy
- Howden School – Amy Orley (Admin and HR Manager / Head's PA) -email dplink@howdenschool.net
- Wolfreton School and Sixth Form College– Sadie Prestwood (Operations Manager and PA to the HT) – email dplink@wolfreton.co.uk

5.4. Any queries in relation to this policy or the handling or personal data within the Trust should be referred to the relevant academy'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.

5.5. 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

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

6.2. 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.)

6.3. 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 (unless reliance on consent is prohibited by EU or Member State law)
- 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

(Please note that this section 7 is only relevant to the extent that the Trust is processing personal data on the grounds of consent and not one of the other processing conditions referred to in section 6 above)

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

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

7.3. Where consent is given, a record must be kept documenting how and when consent was given.

7.4. 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.

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

7.6. Where a child is under the age of 16, the consent of parents/carers will generally be sought 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

8.1. Under DP Legislation, 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 (including but not limited to job applicants, staff, contractors, learners and their families, governors and suppliers).

8.2. 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.

8.3. 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 that the child will understand.

8.4. 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 contact details of 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 outside the European Economic Area 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

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

8.6. 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 are used to communicate with the individual, at the latest, when the first communication takes place.

8.7. 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.

8.8. The Trust does not use automated decision-making processes.

8.9. The Trust does not use personal data for profiling purposes.

9. The right of access

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

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

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

9.4. 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.

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

9.6. 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.

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

9.8. 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 will be extended by a further two months. The individual must be informed of this extension, and receive an explanation of why the extension is necessary, within one month of the receipt of the request.

9.9. 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.

9.10. Any Data User who receives a DSAR should forward it to the DPO immediately (see section 5.2 above) and not respond directly to the request.

9.11. In addition, parents 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 from obtaining a copy of their school records. As part of this process the Trust will apply the appropriate charge for providing copies of records.

10. The right to rectification

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

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

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

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

10.5. 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.

10.6. Any Data User who receives a rectification request should forward it to the DPO immediately (see section 5.2 above) and not respond directly to the request.

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

11.1. Individuals 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

11.2. 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

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

11.4. Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

11.5. 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.

11.6. Any Data User who receives an erasure request should forward it to the DPO immediately (see section 5.2 above) and not respond directly to the request.

12. The right to restrict processing

12.1. Individuals have the right to block or suppress the Trust's processing of personal data in certain limited circumstances.

12.2. 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.

12.3. 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

12.4. 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.

12.5. The Trust will inform individuals when a restriction on processing has been lifted.

12.6. Any Data User who receives a restriction request should forward it to the DPO immediately (see section 5.2 above) and not respond directly to the request.

13. The right to data portability

13.1. Individuals 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.

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

13.3. 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

13.4. 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.

13.5. The Trust will provide the information free of charge.

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

13.7. 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.

13.8. The Trust will respond to any requests for portability within one month.

13.9. 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.

13.10. 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.

13.11. Any Data User who receives a request for portability should forward it to the DPO immediately (see section 5.2 above) and not respond directly to the request.

14. The right to object

14.1. The Trust will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

14.2. Individuals have the right to object to the following:

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

14.3. 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

14.4. Any Data User who receives an objection request should forward it to the DPO immediately (see section 5.2 above) and not respond directly to the request.

15. Privacy by design and privacy impact assessments

15.1. 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.

15.2. 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.

15.3. 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.

15.4. 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.

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

15.6. 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.

15.7. 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

15.8. 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.

15.9. Each DPIA will be overseen by the DPO.

16. Third party data processors

16.1. 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 is required under DP Legislation to enter into a written contract 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.

16.2. 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

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

17.2. The Trust will ensure that all Data Users are made aware of, and understand, what constitutes a data breach.

17.3. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the ICO will be informed.

17.4. All notifiable breaches will be reported to the ICO within 72 hours of the Trust becoming aware of it.

17.5. The risk of the breach having a detrimental effect on the individual, and the need to notify the ICO, will be assessed on a case-by-case basis.

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

17.7. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the ICO.

17.8. Internal reporting procedures are in place at the Trust, which facilitate decision-making in relation to whether the ICO and/or the public need to be notified.

17.9. Within any breach notification, the following information will be outlined in particular:

- 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

17.10. Failure to report a breach when required to do so may result in the Trust receiving a fine, as well as a fine for the breach itself.

17.11. If you become aware of any personal data breach (e.g. a device has been lost or stolen, or any personal data has been disclosed or accessed in error) or personal data being

compromised in any other way, you must report the incident to the DPO immediately (see section 5.2)

18. Data security

18.1. Data Users must not access personal data unless the Trust has given them permission to do so.

18.2. Information about the Trust's staff, learners and others must not be disclosed to any third party or to the person to whom it relates except in accordance with this policy and the Trust's authorised procedures. For example, you must never assume that it is acceptable for a husband to be given personal data about his wife; they may be estranged or simply wish to keep their affairs separate. **In the event that you receive a request from a third party for disclosure of, or to inspect, personal data relating to any individual (including but not limited to staff and learners) you should refer the request to the DPO immediately.** You should make such a referral in all cases and should not respond to the request regardless of the identity of the requestor (including where the requestor is the police or any government agency or public authority) as we have a set procedure for responding to such requests that must be followed.

18.3. Subject to section 18.2 above, if you are in any doubt as to the identity of an individual, you must verify his or her identity before disclosing personal data to him or her.

18.4. Confidential paper records must be kept in a locked filing cabinet, cupboard, drawer or safe, with restricted access. Any keys that you hold in respect of such storage locations must be retained on your person at all times and not left unattended on Trust premises (including overnight).

18.5. Confidential paper records must not be left unattended or in clear view anywhere with general access.

18.6. Paper documents containing confidential information should be disposed of in accordance with the Trust's confidential waste procedures (such as shredding). Digital storage devices should be physically destroyed when no longer required.

18.7. Data Users should ensure that individual monitors do not show personal data to passers-by and that they lock or log off from their computer when it is unattended.

18.8. When sending confidential information by fax or by email, Data Users must always check that the recipient is correct before sending.

18.9. Where appropriate, personal data should be anonymised or pseudonymised.

18.10. Where personal data that could be considered private or confidential is taken off the premises, either in electronic or paper format, Data Users must 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 Trust premises accepts full responsibility for the security of the data.

18.11. Any requests for references that you receive must be referred to your relevant Data Protection Link or the DPO. In particular, you should never provide references for any other individual on social or professional networking sites, as such references (whether positive or negative) can be attributed to us and create legal liability for both us and you as the author

of the reference. References should not be given about an individual to a third party unless that individual has provided consent.

18.12. 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.

18.13. Before sharing data, all Data Users must 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

18.14. Under no circumstances are visitors allowed access to confidential or personal data. Visitors to areas of the Trust containing sensitive information must be supervised at all times.

18.15. Any stranger seen in entry-controlled areas should be reported.

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

18.17. All post received at Trust premises, whether or not marked strictly private and confidential and/or for the attention of an individual Data User, may be opened and inspected prior to distribution. You should be mindful of this if you ask for personal items or correspondence to be delivered to Trust premises.

19. Disclosure and Barring Service ("DBS") data

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

19.2. Data provided by the DBS will never be duplicated.

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

20. Additional information

20.1. This policy does not form part of any employee's contract of employment and it may be amended by the Trust at any time. Any changes will be notified to you in writing.

20.2. 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 5.3 above).

20.3. This policy will be reviewed every year to ensure it is achieving its stated objectives.

THE CONSORTIUM
ACADEMY TRUST

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 Data Protection Link (person as specified in 5.3)