CORINIUM EDUCATION TRUST

Policy: Records Management

Table of Contents:

1. Legal framework

1.1. This policy has due regard to legislation including, but not limited to, the following:
- UK General Data Protection Regulation (GDPR) 2021;
- EU GDPR;
- Data Protection Act 2018;
- Freedom of Information Act 2000;
- Limitation Act 1980 (as amended by the Limitation Amendment Act 1980).

1.2. This policy also has due regard to the following guidance:
- DfE (2023) 'Careers guidance and access for education and training providers'
- ESFA (2022) 'Record keeping and retention information for academies and academy trusts'
- Information Records Management Society (IRMS) (2019) 'Information Management Toolkit for Schools';
- IRMS (2019) 'Academies Toolkit'
- DfE (2018) 'Data protection: a toolkit for schools';
- DfE (2018) 'Careers guidance and access for education and training providers'.

1.3. This policy will be implemented in accordance with the following school policies and procedures:
- Cyber Security Policy
- Data Protection Policy;
- Freedom of Information Policy;
- Retention Log;
- ICT Acceptable Use Policy.

2. Responsibilities

2.1. The Corinium Education Trust is the 'data controller' for all the personal data processed by its schools and by the central team at The Corinium Education Trust.

2.2. The whole Trust has a responsibility for maintaining its records and record-keeping systems in line with statutory requirements. The Trust Lead (CEO) holds the overall responsibility for this policy and for ensuring it is implemented correctly.

2.3. The Data Protection Officer (DPO) is responsible for the management of records at The Corinium Education Trust.

2.4. The DPO at The Corinium Education Trust is Tessa Rollings, Director of Finance and Operations.

2.5. The DPO is responsible for promoting compliance with this policy and reviewing the policy on an annual basis, in conjunction with the Trust Lead (CEO). The DPO is responsible for ensuring that all records are stored securely, in accordance with the retention periods outlined in this policy and are disposed of safely and correctly.

2.6. All staff members are responsible for ensuring that any records they are responsible for (including emails) are accurate, maintained securely and disposed of correctly, in line with the provisions of this policy.

3. Management of pupil records

3.1. Pupil records are specific documents that are used throughout a pupil's time in the education system – they are passed to each school that a pupil attends and include all personal information relating to them, e.g. date of birth, home address, as well as their progress and achievements.

3.2. The following information is stored on the front of a pupil record, and will be easily accessible:
- Forename, surname, and date of birth;
- Unique pupil number;
- Date when the file was opened.

3.3. The following information is stored inside the front cover of a pupil record, and will be easily accessible:
- Any preferred names;
- Emergency contact details and the name of the pupil's doctor;
- Any allergies or other medical conditions that are important to be aware of;
- Names of people with parental responsibility, including their home address(es) and telephone number(s);
- Any other agency involvement, e.g. speech and language therapist;
- Reference to any other linked files.

3.4. The following information is stored in a pupil record, and will be easily accessible:
- Admissions form;
- Details of any SEND;
- If the pupil has attended an 'early years' setting, the record of transfer;
- Data collection or data checking form;
- Annual written reports to parents;
- National curriculum and agreed syllabus record sheets;
- Notes relating to major incidents and accidents involving the pupil;
- Any information about an EHC plan and support offered in relation to the EHC plan;
- Medical information relevant to the pupil's on-going education and behaviour;
- Any notes indicating child protection disclosures and reports;
- Any information relating to exclusions;
- Any correspondence with parents or external agencies relating to major issues, e.g. mental health;
- Notes indicating that records of complaints made by parents or the pupil;
- Examination results – pupil copy;
- SATs results.

3.5. The following information is subject to shorter retention periods and, therefore, will be stored separately in a personal file for the pupil in the school office:
- Attendance registers and information;
- Absence notes and correspondence;
- Parental and, where appropriate, pupil consent forms for educational visits, photographs and videos, etc.
- Accident forms – forms about major accidents will be recorded on the pupil record;
- Consent to administer medication and administration records;
- Copies of pupil birth certificates, passports etc.
- Correspondence with parents about minor issues, e.g. behaviour;
- Pupil work;
- Previous data collection forms that have been superseded.

3.6. Hard copies of disclosures and reports relating to child protection are stored in a sealed envelope, in a securely locked filing cabinet in the school office – a note indicating this is marked on the pupil's file.

3.7. Hard copies of complaints made by parents or pupils are stored in a file in the headteacher's office – a note indicating this is marked on the pupil's file.

3.8. Actual copies of accident and incident information are stored separately on the school's management information system and held in line with the retention periods outlined in this policy – a note indicating this is marked on the pupil's file. An additional copy may be placed in the pupil's file in the event of a major accident or incident.

3.9. The Corinium Education Trust will ensure that no pupil records are altered or amended before transferring them to the next school that the pupil will attend. The only exception is if any records placed on the pupil's file have a shorter retention period and may need to be removed. In such cases, the Headteacher under the guidance of the DPO will remove these records.

3.10. Electronic records relating to a pupil's record will also be transferred to the pupils' next school. Section 12 of this policy outlines how electronic records will be transferred.

3.11. The primary schools will not keep any copies of information stored within a pupil's record unless there is ongoing legal action at the time during which the pupil leaves the school. The responsibility for these records will then transfer to the next school that the pupil attends.

3.12. If any pupil attends Cirencester Deer Park School until statutory school leaving age, the school will keep the pupil's records until the pupil reaches the age of 25 years.

3.13. The Corinium Education Trust's schools will, wherever possible, avoid sending a pupil record by post. Where a pupil record must be sent by post, it will be sent by registered post, with an accompanying list of the files included. The recipient school is required to sign a copy of the list to indicate that they have received the files and return this to the school.

4. Retention of pupil records and other pupil-related information

4.1. The table below outlines The Corinium Education Trust's retention periods for individual pupil records and the action that will be taken after the retention period, in line with any statutory requirements.

4.2. Electronic copies of any information and files will be destroyed in line with the retention periods below.

4.3. For all other records, the retention period should be for the duration of the 'event'/activity, or whilst the pupil remains at school plus one month, whichever is less.

Type of file	Retention period	Action taken after retention period ends
Personal identifiers, contacts and personal characteristics		
Images used for identification purposes	For the duration of the event/activity, or whilst the pupil remains at school, whichever is less, plus one month	Securely disposed of
Images used in displays	Whilst the pupil is at school	Securely disposed of
Images used for marketing purposes	In line with consent period	Securely disposed of
Biometric data	For the duration of the event/activity, or whilst the pupil remains at school, whichever is less, plus one month	Securely disposed of
Postcodes, names and characteristics	Whilst the pupil is at school, plus five years	Securely disposed of
House number and road	For the duration of the event/activity, plus one month	Securely disposed of
Admissions		
Register of admissions [School Admissions Code]	Every entry in the admissions register will be preserved for a period of three years after the date on which the entry was made	Information is reviewed and the register may be kept permanently
Admissions (including in year admissions, where the admission is successful) [School Admissions Code]	Date of admission, plus one year	Securely disposed of
Admissions appeals (where the appeal is unsuccessful) [School Admissions Code]	Resolution of the case, plus one year	Securely disposed of

Proof of address (supplied as part of the admissions process) [School Admissions Code]	Current academic year, plus one year	Securely disposed of
All records relating to the creation and implementation of the Admissions Policy [School Admissions Code]	Life of the policy, plus three years and then review	Securely disposed of
Pupils' educational records		
[Primary schools only] Pupils' educational records [The Education (Pupil Information) (England) Regulations 2005]	Whilst the pupil remains at the school	Retained for a short period to allow for any queries or reports to be completed, before transfer to the next destination.
[Secondary schools only] Pupils' educational records [The Education (Pupil Information) (England) Regulations 2005]	25 years after the pupil's date of birth	Reviewed and securely disposed of if no longer needed
Child protection information held on a pupil's record [KCSIE 2021]	Stored in a sealed envelope for the same length of time as the pupil's record Records also subject to any instruction given by the Independent Inquiry into Child Sex Abuse (IICSA)	Securely disposed of – shredded
Type of file	Retention period	Action taken after retention period ends
Child protection records held in a separate file [KCSIE 2021]	25 years after the pupil's date of birth Records also subject to any instruction given by the IICSA	Securely disposed of – shredded
Attendance		
Attendance registers [School Admissions Code]	Every entry is retained for a period of three years after the date on which the entry was made	Securely disposed of
Correspondence relating to any absence (authorised or unauthorised) [Education Act 1996]	Current academic year, plus two years	Securely disposed of

SEND		
SEND files, reviews and EHC plans, including advice and information provided to parents regarding educational needs and accessibility strategy [Special Educational Needs and Disability Act 2001]	The pupil's date of birth, plus 31 years	Securely disposed of
Extra-curricular activities		
Parental consent forms for school trips where a major incident occurred [Limitation Act 1980]	25 years after the pupil's date of birth on the pupil's record (permission slips of all pupils on the trip will also be held to show that the rules had been followed for all pupils)	Securely disposed of – shredded

5. Retention of staff records

5.1. The table below outlines the school's retention period for staff records and the action that will be taken after the retention period, in line with any statutory requirements.

5.2. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

5.3. For all other records, the retention period should be for the duration of the 'event'/activity, or whilst the staff remains at school plus six months, whichever is less.

Type of file	Retention period	Action taken after retention period ends
Operational		
Staff members' personnel file [Limitation Act 1980]	Termination of employment, plus six years, unless the member of staff is part of any case which falls under the terms of reference of the IICSA. If this is the case, the file will be retained until the IICSA enquiries are complete	Securely disposed of
Pre-employment vetting information (successful candidates) [KCSIE]	For the duration of the employee's employment, plus six years	Securely disposed of
Evidence of right to work in the UK [An employer's guide to right to work checks: 31 August 2021]	Added to staff personnel file or, if kept separately, termination of employment, plus no longer than two years	Securely disposed of
Disciplinary and grievance procedures		
Child protection allegations, including where the allegation is unproven [KCSIE 2021]	Added to staff personnel file, and until the individual's normal retirement age, or 10 years from the date of the allegation – whichever is longer If allegations are malicious, they are removed from personal files If allegations are found, they are kept on the personnel file and a copy is provided to the person concerned unless the member of staff is part of any case which falls under the terms of reference of the IICSA. If this is the case, the file is retained until IICSA enquiries are complete	Reviewed and securely disposed of – shredded

6. Retention of senior leadership and management records

6.1. The table below outlines the school's retention periods for senior leadership and management records, and the action that will be taken after the retention period, in line with any statutory requirements.

6.2. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Governing (including Trustee) boards		
Meeting papers relating to the annual parents' meeting	Date of meeting, plus a minimum of six years	Securely disposed of

7. Retention of health and safety records

7.1. The table below outlines the school's retention periods for health and safety records, and the action that will be taken after the retention period, in line with any statutory requirements.

7.2. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Health and safety		
Records kept under the Control of Substances Hazardous to Health Regulations [Control of Substances Hazardous to Health 2002 (COSHH)]	Date of incident, plus 40 years	Securely disposed of
Information relating to areas where employees and persons are likely to come into contact with asbestos [Control of Asbestos at Work Regulations 2012]	Date of last action, plus 40 years	Securely disposed of
Accident reporting (adults, pupils, and RIDDOR)	Date of accident plus three years	Securely disposed of

8. Retention of financial records

8.1. The table below outlines the school's retention periods for financial records and the action that will be taken after the retention period, in line with any statutory requirements.

8.2. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Payroll and pensions		
Maternity pay records [Statutory Maternity Pay (General) Regulations 1986]	Current academic year, plus three years	Securely disposed of
Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Current academic year, plus six years	Securely disposed of
Contract management		
All records relating to the management of contracts under seal [Limitation Act 1980]	Last payment on the contract, plus 12 years	Securely disposed of
All records relating to the management of contracts under signature [Limitation Act 1980]	Last payment on the contract, plus six years	Securely disposed of

9. Retention of other school records

9.1. For all other records, the overriding principle to consider in relation to data retention is that **"personal data must not be retained for longer than is necessary for its lawful purpose"** (GDPR).

10. Retention of emails

10.1. Group email addresses will have an assigned member of staff who takes responsibility for managing the account and ensuring the correct disposal of all sent and received emails. All staff members with an email account will be responsible for managing their inbox.

10.2. Emails can act as evidence of the school's activities, i.e. in business and fulfilling statutory duties, so all relevant emails, e.g. invoices, will be retained for at least 12 months.

10.3. The Corinium Education Trust's expectations of staff members in relation to their overall conduct when sending and receiving emails is addressed in the school's Online Safety Policy. All emails should be deleted after 2 years, unless stated otherwise.

10.4. Correspondence created by the SLT and other members of staff with administrative responsibilities will be retained for three years before being reviewed and, if necessary, securely disposed of.

10.5. Personal emails, i.e. emails that do not relate to work matters or are from family members, will be deleted as soon as they are no longer needed. Staff members will review and delete any emails they no longer require at the end of every academic year.

10.6. Staff members will not, under any circumstances, create their own email archives, e.g. saving emails on to personal hard drives. Staff members will be aware that the emails they send could be required to fulfil a subject access request (SAR) or freedom of information (FOI) request. Emails will be drafted carefully, and staff members will review the content before sending.

10.7. Individuals, including children, have the right to submit an SAR to gain access to their personal data to verify the lawfulness of the processing – this includes accessing emails.

10.8. All SARs will be handled in accordance with the school's Data Protection Policy. FOI requests will be handled in accordance with the school's Freedom of Information Policy.

10.9. When handling a request for information, the DPO will speak to the requestor to clarify the scope of the request and whether emails will be required to fulfil the SAR or FOI request. Where an SAR has been made electronically, the information will be provided in a commonly used electronic format. All requests will be responded to without delay and at the latest, within one month of receipt.

10.10. If a request is manifestly unfounded, excessive or repetitive, a fee will be charged. All fees will be based on the administrative cost of providing the information.

10.11. Where a request is manifestly unfounded or excessive, the school 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.

10.12. Staff members will discuss any queries regarding email retention with the DPO.

11. Identifying information

11.1. Following the release of the EU's General Data Protection Regulation (EU GDPR), the UK's Data Protection Act 2018 (DPA 2018) and the subsequent UK General Data Protection Regulation (UK GDPR) entitles all individuals to have the right to data minimisation and data protection by design and default – as the data controller, The Corinium Education Trust (and schools within The Corinium Education Trust) ensures appropriate measures are in place for individuals to exercise this right.

11.2. Wherever possible, the school uses pseudonymisation, also known as the 'blurring technique', to reduce the risk of identification.

11.3. Once an individual has left the school, if identifiers such as names and dates of birth are no longer required, these are removed or less specific personal data is used, e.g. the month of birth rather than specific date – the data is blurred slightly.

11.4. Where data is required to be retained over time, e.g. attendance data, the school removes any personal data not required and keeps only the data needed – in this example, the statistics of attendance rather than personal information.

12. Storing and protecting information

12.1. The DPO will undertake a business impact assessment to identify which records are vital to school management and these records will be stored in the most secure manner. The schools will conduct a back-up of information on a termly basis to ensure that all data can still be accessed in the event of a security breach, e.g. a virus, and prevent any loss or theft of data.

12.2. Where possible, backed-up information will be stored off the school premises, using a central back-up cloud service operated by the Local Authority (LA). The DPO will ensure that the location of the cloud storage and the security offered is appropriate for the information and records stored on it.

12.3. Confidential paper records are kept in a locked filing cabinet, drawer or safe, with restricted access. Any room or area where personal or sensitive data is stored will be locked when unattended. Confidential paper records are not left unattended or in clear view when held in a location with general access.

12.4. 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. Where data is saved on removable storage or a portable device, the device is kept in a locked and fireproof filing cabinet, drawer or safe when not in use. Memory sticks are not used to hold personal information unless they are password-protected and USB sticks are fully encrypted.

12.5. 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. Staff and governors do 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 regularly prompts users to change their password.

12.6. Emails containing sensitive or confidential information are password-protected or sent via a secure encrypted or data transfer system to ensure that only the recipient is able to access the information. The password will be shared with the recipient in a separate email. Personal information is never put in the subject line of an email. Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

12.7. When sending confidential information by fax, members of staff always check that the recipient is correct before sending.

12.8. Where personal information that could be considered private or confidential is taken off the premises, to fulfil the purpose of the data in line with the UK GDPR, either in an electronic or paper format, The Corinium Education Trust's staff 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 school premises accepts full responsibility for the security of the data.

12.9. If documents that have been taken off the school premises will be left unattended, the staff member will leave the documents in the locked boot of a car or keep them on their person. A record will be kept of any document that is taken off the school premises that logs the location of the document and when it is returned to the school site, this includes records that are digitally remotely accessed.

12.10. Before sharing data, staff always ensure that:
- The Trust/school has adequate and recorded consent from data subjects to share it;
- The Trust/school has adequate security is in place to protect the individual's data;
- The data recipient has been outlined in a privacy notice.

12.11. The Corinium Education Trust has data sharing agreements with all data processors and third parties with whom data is shared. These agreements are developed by the DPO and cover information about issues such as access controls and permissions.

12.12. A record is kept of what level of access each staff member has to data. This record details information including:
- What level of access each staff member has;
- Limits on how staff members access data;
- What actions staff members can perform;
- What level of access is changed or retained when a staff member changes role within the Trust/school;
- Who can authorise requests to change permissions and access.

12.13. All staff members implement a 'clear desk policy' to avoid unauthorised access to physical records containing sensitive or personal information. All confidential information is stored in a securely locked filing cabinet, drawer or safe with restricted access.

12.14. 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.

12.15. Staff are required to use their school login details to use photocopiers and printers.

12.16. The physical security of the school's buildings and storage systems, and access to them, is reviewed at least annually by the site manager in conjunction with the DPO. If an increased risk in vandalism, burglary or theft is identified, this will be reported to the Trust Lead (CEO) and/or individual school's headteacher and extra measures to secure data storage will be put in place.

12.17. All systems that allow staff and pupils to remotely access information from the school's network whilst they are not physically at the school have strong security controls in place which are reviewed at least annually by the DPO.

12.18. The DPO decides what restrictions are necessary to prevent information or records being downloaded, transferred or printed while the user is not on the school site.

12.19. The school takes its duties under the UK GDPR seriously and any unauthorised disclosures may result in disciplinary action.

12.20. The DPO is responsible for ensuring continuity and recovery measures are in place to ensure the security of protected data. Any damage to or theft of data will be managed in accordance with the school's Data and E-Security Breach Prevention and Management Plan.

12.21. As a result of the UK's departure of the European Union (EU),on 1 January 2021, data controllers and processors follow the UK GDPR, and the Data Protection Act 2018, where:
- As UK data controllers, they collect, store or process the personal data of individuals residing in the UK;

- As non-UK data controllers, they offer goods or services to, or monitor the behaviour of, UK residents.

12.22. Data controllers and processors must follow the EU GDPR where:
- They collect, store or process the personal data of individuals residing in the EU;
- As non-EU data controllers, they offer goods or services to, or monitor the behaviour of, EU residents.

13. Accessing information

13.1. We are transparent with data subjects, the information we hold and how it can be accessed.

13.2. All members of staff, parents of registered pupils and other users of the school, e.g. visitors and third-party clubs, are entitled to:
- Know what information the school holds and processes about them or their child and why.
- Understand how to gain access to it.
- Understand how to provide and withdraw consent to information being held.
- Understand what the school is doing to comply with its obligations under the UK GDPR.

13.3. All members of staff, parents of registered pupils and other users of the school and its facilities have the right, under the DPA (2018) and/or UK GDPR, to access certain personal data being held about them or their child.

13.4. Personal information can be shared with pupils once they are considered to be at an appropriate age and responsible for their own affairs; although, this information can still be shared with parents. Pupils who are considered by the school to be at an appropriate age to make decisions for themselves are entitled to have their personal information handled in accordance with their rights.

13.5. The school will adhere to the provisions outlined in the school's Data Protection Policy when responding to requests seeking access to personal information

14. Digital continuity statement

14.1. Digital data that is retained for longer than six years will be identified by the DPO and named as part of a Digital Continuity Statement. The data will be archived to dedicated files on the school's server, which are password-protected – this will be backed-up in accordance with Section 12 of this policy.

14.2. Memory sticks are never used to store digital data, subject to a Digital Continuity Statement.

14.3. The ICT technician will review new and existing storage methods annually and, where appropriate, add them to the digital continuity statement.

14.4. The following information will be included within the Digital Continuity Statement:
- A statement of the business purposes and statutory requirements for keeping the records;
- The names of the individuals responsible for long term data preservation;
- A description of the information assets to be covered by the digital preservation statement;
- A description of when the record needs to be captured into the approved file formats;
- A description of the appropriate supported file formats for long-term preservation;
- A description of the retention of all software specification information and licence information;
- A description of how access to the information asset register is to be managed in accordance with the UK GDPR.

15. Information audit

15.1. The Corinium Education Trust conducts information audits on an ad hoc basis against all information held by the school to evaluate the information the school is holding, receiving and using, and to ensure that this is correctly managed in accordance with the UK GDPR.

15.2. As a minimum, The Corinium Education Trust will seek to do an annual audit, normally 3 months after the end of the academic year to allow Schools time to do relevant house-keeping before the audit.

15.3. This includes the following information:

- Paper documents and records;
- Electronic documents and records;
- Databases;
- Microfilm or microfiche;
- Sound recordings;
- Video and photographic records;
- Hybrid files, containing both paper and electronic information;
- Apps and portals.

15.4. The information audit may be completed in a number of ways, including, but not limited to:

- Interviews with staff members with key responsibilities – to identify information and information flows, etc.
- Questionnaires to key staff members to identify information and information flows, etc.
- Spot checks to ensure data is being stored in the appropriate format for the appropriate amount of time;
- A mixture of the above.

15.5. The DPO is responsible for completing the information audit. The information audit will include the following:

- The school's data needs;
- The information needed to meet those needs;
- The format in which data is stored;
- How long data needs to be kept for;
- Vital records status and any protective marking;
- Who is responsible for maintaining the original document.

15.6. The DPO will consult with staff members involved in the information audit process to ensure that the information is accurate.

15.7. Once it has been confirmed that the information is accurate, the DPO will record all details on the school's Data Asset Register.

15.8. An information asset owner is assigned to each asset or group of assets. They will be responsible for managing the asset appropriately, ensuring it meets the school's requirements, and for monitoring risks and opportunities.

15.9. The information displayed on the Data Asset Register will be shared with the headteacher to gain their approval.

16. Disposal of data

16.1. Where disposal of information is outlined as standard disposal, this will be recycled appropriate to the form of the information, e.g. paper recycling, electronic recycling.

16.2. Where disposal of information is outlined as secure disposal, this will be shredded or pulped. Electronic information will be scrubbed clean and, where possible, cut, archived or digitalised. The DPO will keep a record of all files that have been destroyed.

16.3. Where the disposal action is indicated as reviewed before it is disposed, the DPO will review the information against its administrative value – if the information should be kept for administrative value, the DPO will keep a record of this.

16.4. If, after the review, it is determined that the data should be disposed of, it will be destroyed in accordance with the disposal action outlined in this policy.

16.5. Where information has been kept for administrative purposes, the DPO will review the information again after three years and conduct the same process. If it needs to be destroyed, it will be destroyed in accordance with the disposal action outlined in this policy. If any information is kept, the information will be reviewed every three subsequent years.

16.6. Where information must be kept permanently, this information is exempt from the normal review procedures.

16.7. Records and information that might be of relevant to the Independent Inquiry into Child Sexual Abuse (IICSA) will not be disposed of or destroyed.

17. Monitoring and review

17.1. This policy will be reviewed on an annual basis by the DPO in conjunction with the the Trust's Executive Team and Trustees.

17.2. Any changes made to this policy will be communicated to all members of staff and The Corinium Education Trust's Trustees' Board.

Document History

Creation Date November 2021

Trust Lead Director of Finance and Operations

Approved by Trustees

First approval date Oct 2022

Review frequency Annually

Review date	Significant amendments	Made by	Next review
Oct 2021	New policy based on a template from The School Bus to reflect UK GDPR. Reviewed and edited by Andy Tate (DFO) and Trustee Mark Harwood-James	AXT MHJ	Oct 2022
Nov 2022	No significant changes made other than the name of the Trust's DFO. This role will be reviewed in 2023-24. Policy checked against Data protection and ICT Acceptable Use Policy for accuracy. Minor corrections to grammar.	CXH MHJ	Nov 2023
Nov 2023	DFO role to be reviewed in 2024-2025 (with regards to outsourcing). Checked against The School Bus model policy and minor updates made, including addition of 'personal identifiers, contacts and characteristics.'	CXH TJR	Nov 2024