Centre Academy East Anglia

Privacy Notice (Data Protection Policy)

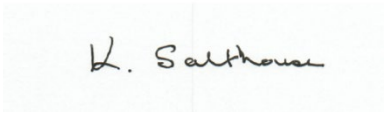
Equality Statement

Centre Academy East Anglia is committed to a policy of equality and aims to ensure that no employee, job applicant, pupil or other member of the school community is treated less favourably on grounds of sex, race, colour, ethnic or national origin, marital status, age, sexual orientation, disability or religious belief. We provide a safe, supportive and welcoming environment

To be reviewed annually Next review date: March 2020

Signed: **Date: 23/03/19**

Principal and CEO **Dr Rollo**



Signed: **Date: 23/03/19**

Head of School **Mrs Salthouse**

Centre Academy East Anglia is committed to safeguarding and promoting the welfare of children and young people and expects all staff to share this commitment.

1. Introduction

Centre Academy East Anglia (CAEA) is a data controller (ICO Registration Number: Z7451143) and takes its data protection responsibilities seriously. The School recognises the need to protect the personal data with which it is provided and to process it legally.

This Privacy Notice and Data Protection Policy provides detailed information to explain how CAEA processes personal data and applies regardless of whether it is in paper or electronic format. Questions regarding personal data or its use should be directed to the Data Manager through the School Office.

1.1 Contents

1.2 Legal Framework

This document considers all relevant legislation and guidance, including, but not limited to:

Human Rights Act, 1998
The Freedom of Information Act, 2000
Safeguarding Vulnerable Groups Act, 2006
The Childcare (Disqualification) Regulations, 2009
The Education (Independent School Standards) Regulations, 2014
Working Together to Safeguard Children, 2015
General Data Protection Regulation (GDPR), 2018
DfE Data Protection: toolkit for schools, 2018
ICO Guide to the General Data Protection Regulations, 2018

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

1.3 Data Manager

The Head of School will be the designated Data Manager for CAEA. The Data Manager will review this and other Data Policies and Procedures on an annual basis. All questions or concerns sent to the School Office about Personal Data, including Freedom of Information or Data Access Requests will be forwarded to the Data Manager. The Data Manager will also be the point of contact with the ICO in the event of Data Breaches.

The Data Manager will provide an annual report of their activities directly to the Governance and, where relevant, report their advice and recommendations on school data protection issues.

2. Categories of Information Held

2.1 Personal Data

CAEA needs to process personal data about individuals connected to or visiting the School including prospective, current and past pupils (together with their parents or carers), staff, suppliers and contractors.

The personal data may take different forms including factual information, expressions of opinion and images or other recorded information. Examples include:

- personal information (e.g. names, contact details and gender)
- family details
- emergency contact information
- admissions, academic, disciplinary and other related records, including information about:
    - special educational needs
    - assessments and examinations
    - attendance and absences
    - references
- education, qualification and employment data
- contract information
- images, audio and video recordings
- financial information
- courses, meetings or events attended

2.2 Special Category Personal Data and Criminal Offence Data

As well as personal data, the School also needs to process special category personal data (e.g. concerning health, ethnicity or religion) and criminal records information about some individuals (particularly pupils and staff). This is done in accordance with applicable law (including with respect to safeguarding or employment) or by explicit consent.

3. Collecting Personal Data

CAEA collects most of the personal data it processes directly from the individual concerned (or in the case of pupils, from their parents). In some cases, the school collects data from third parties (for example, referees, previous schools, the Disclosure and Barring Service, or professionals or authorities working with the individual) or from publicly available resources. Whilst the vast majority of information is mandatory, some may be provided on a voluntary basis. Please see section 3.3 for more information.

3.2 Purpose for Collecting Personal Data

CAEA requires personal data in order to function as an Independent Special Needs School. More specifically, the School collects and uses individual data for the following reasons:

3.2.1 Selection and enrolment of new students or recruitment of new staff

3.2.2 Student learning and progress, including:

Administering the curriculum; monitoring pupil progress; managing discipline; monitoring and managing student's special educational needs; provision of IT in accordance with IT policies; reporting progress internally, to parents and to regulatory bodies; administration of examination entries and publishing results; providing references for pupils, medical records.

3.2.3 Pastoral care, therapeutic care, welfare and student safeguarding, including:
Administering SEN provision and therapy support; monitoring pastoral targets.

3.2.4 Operational management, including:
Administration of invoices, fees and accounts; the management of School property; the management of security and safety (including use of CCTV and monitoring of the School's IT and communications systems); assessment of the quality of services (including enabling the monitoring of selected protected characteristics); the implementation of School's policies and procedures

3.2.5 Staff administration, development and deployment, including:

Administration of sick leave, payroll, healthcare and pensions; management of the staff performance management process; management of complaints, capability or disciplinary procedures; maintenance of records for current and previous staff; providing references

3.2.6 Statutory and legal compliance, including:

Submission of annual census information; preparation of information for inspectoral bodies; sharing information with relevant authorities

3.2.7 Promotion of the School, through various communication platforms include the School website and prospectus and any other internal/external brochures.

3.2.8 Maintenance of relationships with the wider school community by communicating with current and former pupils and/or their parents about upcoming events and activities

3.3 Lawful Basis for Data Processing

With the exception of data collected under sections 3.2.7 and 3.2.8, the personal data above is collected in order to fulfil CAEA's public tasks and legal obligations (including those under parental and staff employment contracts). CAEA recognises these purposes also form its legitimate interests.

Consent will be sought for data collected under sections 3.2.7 and 3.2.8. For current students, consent is sought from parents on the schools admission forms. For staff and other individuals,

if required, consent will be sought at the start of the contract. Should an individual wish to change their consent they can do this at any time through the School Office.

For information about the School's lawful basis for collecting Special Category Personal Data or Criminal Offence Data, please see section 2.2.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services).

3.3.1 Keeping in Touch with Former Students

When requested, CAEA keeps in touch with former students for the purpose of inviting them into school for events. If former students would like to be added to this list, or if they would like to be removed from this list, they should inform the School Office.

4. Handling and Sharing Data

Personal data held by CAEA is processed by appropriate members of staff for the purposes for which the data was provided. The School takes appropriate technical and organisational steps to ensure the security of personal data, these steps are set out in the School's Data Policies and Procedures.

4.1 How Data is Stored

Some of CAEA's systems are provided by third parties, e.g. hosted databases, school websites, the homework portal and cloud storage providers. This is always subject to contractual assurances that personal data will be kept securely and only in accordance with specific directions.

CAEA does not store or transfer personal data outside the European Economic Area unless satisfied that the personal data will be afforded an equivalent level of protection.

4.2 Who We Share Personal Data With

As part of school business, data (including special category personal data where appropriate) is routinely shared with third parties such as:

- examination boards
- the school's professional advisors
- schools or workplaces attended after leaving CAEA
- relevant authorities (e.g. Local Education Authorities, Local Safeguarding Boards, Child or Adult Social Care, Youth Services, DBS, UK Visas and Immigration, Ofsted, HM Revenue and Customs, Department for Education and Department for Work and Pensions, Medical Authorities)

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

For information about CAEA's legal basis for sharing data please see section 3.3.

The School does not otherwise share personal data with, or sell personal data to, other organisations for their own purposes.

5. Retention Periods

CAEA retains personal data only for a legitimate and lawful reason and only for so long as necessary or required by law. Questions about the School's record retention periods for specific data should be directed to the School Office.

For Data security and storage of records (staff) please see appendix 1.7
CAEA takes reference from:
Records Management from the Information and Records Management Society.

6. Your Rights

6.1 Access to Your Personal Data

Under data protection legislation individuals have the right to request access to their information held by CAEA. They also have, in certain cases, the right to request their data be erased, amended or to ask CAEA to stop its processing. This right is subject to certain exemptions and limitations.

6.1.1 Updating Personal Data

CAEA tries to ensure that all personal data is up to date and accurate. The School Office should be notified of any significant changes to important information, such as contact details, as soon as possible.

6.2 Additional Rights

Individuals also have the right to:

- Object to the processing of personal data that is likely to cause, or is causing, damage or distress.
- Prevent processing for the purpose of direct marketing.
- Object to decisions being taken by automated means.
- Claim compensation for damages caused by a breach of the Data Protection regulations.

6.3 Data Protection Requests (Subject Access Requests)

If an individual has any concerns about how CAEA is processing their data, would like access to their data or would like their personal data to be transferred to another person or organisation, they should contact the School Office. Please see Appendix 1.8

Please be aware if raising concerns about the processing of data, the School may have another lawful reason to process the personal data even without consent. This reason will either have been given in this Privacy Notice or exist as part of a contract or agreement (e.g. an employment or parent contract).

CAEA will respond to requests as soon as is reasonably practicable within statutory time-limits. This is one month in the case of requests for access to information, although the School will be able to respond more quickly to smaller or more targeted requests. If the request is excessive or similar to previous requests, CAEA may ask the individual to reconsider or, where Data Protection Law allows, charge a fee. (Please see appendix 1.9 – Access to Personal Data Request)

Certain data is exempt from the right of access. This may include information which identifies other individuals, or information which is subject to legal privilege. CAEA is also not required to disclose any pupil examination scripts, nor any confidential reference given by the school for the purposes of the education, training or employment of any individual, which might cause serious harm to the physical or mental health of the pupil or another individual, would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests, is contained in adoption or parental order records or is given to a court in proceedings concerning the child.

7. Pupil Data

Rights under Data Protection legislation belong to the individual to whom the data relates. However, CAEA will often rely on parental consent to process personal data relating to students (if consent is required) unless, given the nature of the processing in question, and the student's age and understanding, it is more appropriate to rely on the student's consent. Parents should be aware that in such situations they may not be consulted, depending on the circumstances, interests of the child and the parents' legal rights and contract. (please see Appendix 1.8.1)

In general, although student information is always considered to belong to the student, CAEA assumes that their consent is not required for ordinary disclosure of their personal data to their parents, e.g. for the purposes of keeping parents informed about activities, progress and behaviour, and in the interests of the student's welfare, unless, in the school's opinion, there is a good reason to do otherwise.

However, where a student seeks to raise concerns with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents, the school may be under an obligation to maintain confidentiality unless there is a good reason to do otherwise; for example, where the school believes disclosure will be in the best interests of the student or other students or is required by law.

Students can make Subject Access Requests for their own personal data, provided that they have sufficient maturity to understand the request they are making. A student of any age may ask a parent or other representative to make a Subject Access Request on their behalf. Depending on age, maturity and data requested the student's consent or authority may need to be sought by any parent making such a data access request.

8. Data Protection Concerns

Concerns about the way CAEA is collecting or using personal data, concerns that the school has not complied with this policy or concerns that CAEA has not acted in accordance with Data Protection Law, should be raised with the School Office. Alternatively, the Information Commissioner's Office (ICO) can be contacted through https://ico.org.uk/concerns/.

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the Data Manager. If staff receive such a request, they must immediately forward it to the Data Manager.

8.1 Photographs and Videos and CCTV

As part of our school activities, we may take photographs and record images of individuals within our school. (Please see Photography, Video and CCTV Policy)

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the Data Manager.

For more information please refer to our Data Policies and Procedures on use of photographs and videos and CCTV procedures.

8.2 Data Breaches

Steps taken in case of a data breach are set out in the School's Data Protection Data Breach Policy.

8.3 Training

All staff and Governance are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

This Policy should be read in conjunction with the following policies:
Data Protection Data Breach Policy
Data Policies and Procedures
E- Safety (online Safeguarding Policy)
Data Protection – Practical Document for Staff
Freedom of Information Act Policy
Reference to: Records Management from the Information and Records Management Society

Appendix 1: Definitions

Appendix 1.1: Data Controller

A person or organisation that determines the purposes and the means of processing personal data.

Appendix 1.2: Personal Data

Personal data is information which relates to a living individual who can be identified from that data. This may include an individual's name (including initials) or identification number, it may also include factors specific to the individual's physical, cultural or social identity.

Appendix 1.3: Special Category Personal Data

Special category data is more sensitive, so requires more protection. Special category data includes information such as an individual's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics, health, sex life or sexual orientation.

Appendix 1.4: Data Processing

Processing data means obtaining, recording or holding data. It also means carrying out an operation on the data e.g. changing, using, sharing or deleting the data. This could be a manual or automated process.

Appendix 1.5: Lawful Bases for Processing

The lawful bases for processing personal data are set out in Article 6 of the GDPR. At least one must apply whenever personal data is processed.

1.5.1 **Consent**: the individual has given clear consent for their personal data to be processed for a specific purpose.

1.5.2 **Contract**: the processing is necessary for a contract with the individual.

1.5.3 **Legal obligation**: the processing is necessary to comply with the law.

1.5.4 **Vital interests**: the processing is necessary to protect someone's life.

1.5.5 **Public task**: the processing is necessary for a task in the public interest or for official functions, and the task or function has a clear basis in law.

1.5.6 **Legitimate interests**: the processing is necessary for legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Appendix 1.6: Data Breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Appendix 1.7: Data Security and storage of Records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office

- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governance who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our E-Safety (Online Safeguarding Policy/ICT Acceptable Use Agreement/CAEA Handbook for Faculty Staff/ Staff Procedures and Policies.)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected

Appendix 1.8.1 Children and Subject Access Requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Appendix 1.8.2 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

Appendix 1.9

ACCESS TO PERSONAL DATA REQUEST

(Subject Access Request – SARS)

DATA PROTECTION ACT 1998 (Section 7)

Enquirer/s Surname:		**Enquirer's Forenames:**	
Enquirer's Address:			
Enquirer's Postcode:		**Enquirer's Tel No:**	
Enquirer's Email:			
Are you the person who is the subject of the records you are enquiring about (i.e. the "Data Subject")?			**YES / NO**
If NO,			
Do you have parental responsibility for a child who is the "Data Subject" of the records you are enquiring about?			**YES / NO**
If YES,			
Name of child or children about whose personal data records you are enquiring			
Description of Concern/Area of Concern			
Description of Information or Topic(s) Requested (In your own words)			

Additional Information	

Appendix 1.9

Please dispatch Reply to: (*if different from enquirer's details as stated on this form*)

Name

Address

Postcode

DATA SUBJECT DECLARATION

I request that the School search its records based on the information supplied above under Section 7 (1) of the Data Protection Act 1998 and provide a description of the personal data found from the information described in the details outlined above relating to me (or my child/children) being processed by the School.

I agree that the reply period will commence when I have supplied sufficient information to enable the School to perform the search.

I consent to the reply being disclosed and sent to me at my stated address (or to the Despatch Name and Address above who I have authorised to receive such information).

Signature of "Data Subject" (or Subject's Parent) _____

Name of "Data Subject" (or Subject's Parent) (PRINTED)
_____

Dated _____