Data Protection and Information Security Policy

(incl Separated Parents Policy, Data in Transit policy, Special Category Data policy & CCTV policy)

Believing in Excellence means that the Trust has key values that all members of our schools' community live by.

These are:

- Respect;
- Resilience;
- Responsibility.

Date of Policy	January 2022
Date agreed by Trustees	February 2022
Date of next review	March 2024

Contents

Data Protection and Information Security Policy

1. Introduction

Cavendish Education Trust collects and uses personal information about staff, pupils, parents or carers and other individuals who come into contact with the trust. This information is gathered in order to enable it to provide education and other associated functions. In addition, there is a legal requirement to collect and use information to ensure that the trust complies with its statutory obligations.

2. Definitions

Data Protection legislation places obligations on all those who process personal data and defines the following roles:-

Data Controller – the Trust, as the Trust determines the purpose of processing i.e. decides how and why data is used.

Data Processors – the person or organisation that processes data on behalf of the controller. The trust is sometimes a data processor.

Data Subjects – the individuals whose information is collected and processed (for example pupils. parents, carers, members of staff)

ICO – Information Commissioner's Office

3. Registration

The Trust, as a data controller, has to register with the ICO and maintain a record of the information it holds and the purposes for which it obtains and uses personal data (including disclosure in any form to third parties). These details must be kept up to date and available for inspection by the Information Commissioner's Office.

4. The Information Commissioner

The Information Commissioner is the body that oversees compliance with Data Protection legislation, and has powers to force organisations to process personal data lawfully.

Where a data subject is unhappy with some aspect of the processing of their personal information they have the right to complain to the Information Commissioner.

It is recommended that any such issue should be resolved locally between the Trust and the individual concerned where possible. Any enquiries subsequently received from the Information Commissioner will be referred to the Trust's Data Protection Officer.

5. Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with Data Protection, and other related legislation. It applies to information held and processed by the Trust regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

6. Policy statement:

Cavendish Education Trust is committed to ensuring that all information is collected, processed, maintained and disclosed in accordance with the principles that personal data will be:

- processed lawfully, fairly and in a transparent manner
- collected and used for specified, explicit and legitimate purposes
- adequate, relevant and limited to what is necessary for the purpose for processing (‘*data minimisation’*)
- accurate and where required, rectified without delay (‘*accuracy*’)
- not be kept in an identifiable form for longer than necessary (‘*storage limitation’*)
- information must be appropriately secured/protected against unauthorised or unlawful processing, accidental loss, destruction or damage using appropriate technical or organisational measures (‘*integrity and confidentiality’*). This includes:
  – *using appropriate means of transmitting data*
  – *secure storage / disposal of personal information*
  – *where processing is sub-contracted or outsourced (e.g. payroll, disposal of confidential waste paper) there must be suitable Data Protection clauses in the contract*

Personal information must also:

- be processed in accordance with the rights of data subjects e.g. right of access, right of erasure, rectification, restriction, portability and the right to object to certain processing (see section 12)
- not be transferred to countries outside the European Economic Area without adequate protection

7. General Statement

The trust is committed to maintaining the above principles at all times. Therefore, the trust will:

- Inform individuals why the information is being collected when it is collected
- Inform individuals when their information is shared, and why and with whom it was shared
- Check the quality and the accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests
- Ensure our staff are aware of and understand our policies and procedures

8. Responsibilities

All employees, trustees, governors and any other individual handling personal information on behalf of the trust have a responsibility to ensure that they comply with Data Protection legislation and the trust’s policies.

9. The legal basis

The trust must comply with all relevant UK and European Union legislation, including:

- Human Rights Act 1998
- Data Protection Legislation (Data Protection Act 1998, General Data Protection Regulation (GDPR), Data Protection Act 2018)
- Freedom of Information Act 2000
- Common law duty of confidence
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- Health and Safety at Work Act 1974
- Privacy and Electronic Communications (EC Directive) Regulations 2003

10. Information and data definitions

Information is the product of a collection of data and expressed views and opinions based upon it. It can be held and used in many forms including, but not limited to, electronic records, hard copy (paper, fiche) phone calls and conversations. For the purpose of this policy information and data can be regarded as being the same.

This policy relates primarily to any personal data i.e. data relating to individuals or personally identifiable data.

- **Personally Identifiable data** is any data relating to an individual ('data subject) who can be identified directly or indirectly by an identifier such as name, ID number, unique pupil number, location data (e.g. address), online identifier (e.g. IP address) or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.
- **Special Category Data** is sensitive personal data (which requires extra protection) and includes any information that may identify an individual's:
    - racial or ethnic origin,
    - political opinions,
    - religious or philosophical beliefs,
    - trade union membership,
    - health,
    - sex life/orientation
    - genetic/biometric identifier

  Information that is **confidential** but doesn't relate to an individual or individuals includes the following:

  - Trust business or corporate records containing organisationally or publicly sensitive information
  - Any commercially sensitive information such as information relating to commercial proposals or current negotiations
  - Politically sensitive information
  - Information relating to security, investigations and proceedings
  - Any information which, if released, could cause problems or damage to individuals, the public, the trust or another organisation. This could be personal, financial, reputation or legal damage.

11. Data Protection by Design

Whenever a new system or database involving personal data is proposed a Data Protection Impact Assessment (DPIA) will be completed. This will be used to identify and reduce any risks

to privacy and potential risks of harm to individuals through the misuse of their personal information.

12. Data Subject Rights

Any person wishing to exercise their rights under data protection legislation can do so by emailing or writing to the trust; office@cavendish.e-sussex.sch.uk

Requests will be processed within 1 month of receipt of the request, unless the request is complex (or if multiple requests are received from the same person)

Examples of when a request may be considered complex:

- it involves retrieval and appraisal of information from multiple sources
- it involves the retrieval of large volumes of information for one data subject which are difficult to separate from information relating to other data subjects
- it is one in a series of requests from the same individual
- it involves the release of third party data for which consent has been refused or cannot be obtained

In these cases, a 3 month deadline for responding to the request will apply. For complex requests likely to take over 1 month, the applicant will be notified of this within the initial 1 month period.

Right of Access

Under data protection legislation every individual has the right of access to information relating to them. This right is called Subject Access. Any person wishing to make a Subject Access request can do so by following the instructions above. Personal information will never be disclosed verbally in response to a request.

Written consent will always be required from any person nominating a third party to request information on their behalf. Parents may make requests on behalf of their children but if the child is 13 years or older, the child must also provide written consent for the parent to make the application on their behalf.

A nominated person may make an application on behalf of anyone lacking mental capacity who would otherwise have the right to request access to their records. In these circumstances, the person making the application must have proof of a valid Lasting Power of Attorney or an Enduring Power of Attorney or proof of Court-appointed Deputyship.

No information relating to any other person (other than the individual requesting the information) will be disclosed as part of a subject access disclosure.

Any information that may prejudice the prevention and detection of crime may be exempted from disclosure. There are also a number of other exemptions which may be applied and these will be explained on an individual basis.

Right of erasure

This right allows individuals to request that their personal data is deleted where there is no justification for its continued use. It only applies, however, when:

1. The data is no longer necessary for the reason(s) for which it was originally collected
2. The data subject provided consent for the trust to process their data but has subsequently withdrawn this consent

3. That data subject has objected to the trust processing their data and there are no overriding grounds for continuing to process it
4. The data was processed in breach of the GDPR i.e. it was unlawfully processed
5. There is a legal requirement to erase the data
6. The data was collected with parental consent when the data subject was a child and they no longer wish for their data to be held

The trust will also decline a request for erasure:

1. When we have a legal obligation or it is part of our official authority to process the data
2. For public health reasons
3. For certain archiving activities
4. When we need the data in connection with a legal claim

Right to rectification

If data subjects believe that any of the personal data the trust holds about them is inaccurate or incomplete they are entitled to ask for it to be rectified. This will be looked at in the context of why the trust is processing the information any necessary steps will be taken to supplement the information held in order to make it complete.

Right to restriction

In certain circumstances data subjects have a right to request that we temporarily restrict processing and access to their data. This will apply:

1. Whilst establishing accuracy of data, if a data subject has contested this
2. Whilst we follow up any objection raised by a data subject to the trust processing their data.
3. When data has been processed unlawfully but the data subject does not want us to erase it and have asked, instead, for us to restrict processing of the data.
4. When we no longer need the data but the data subject has advised us that they need it in connection with a legal claim.

The right to restrict data doesn't apply if:

1. The processing is necessary for the trust in connection with a legal claim
2. It is necessary for the protection of another person
3. There are substantial public interest reasons for continuing to process the data

Right to portability

Data subjects have a right to request that their data be transferred electronically to another organisation.

This only applies when:

1. The data subject themselves supplied the information and provided consent for the processing; or
2. The data is being processed as part of a contract to which the data subject is party; and
3. The data is held electronically (not in paper files)

Right to object

Data subjects have the right to object to their information being processed in the following circumstances:

- If the trust has decided that processing is necessary either to
  a) perform a task carried out in the public interest or
  b) as part of the trust's official authority or legitimate interest and the data subject feels this is not applicable.
  Information about why the trust is processing information (the legal justification) can be found in the trust's privacy notice.
- If the trust retains information in defence or potential defence of a legal claim but the data subject believes there are insufficient grounds to do so.

Data subjects also have a right to object to their data being used for direct marketing purposes at any time and the trust will cease processing for this purpose if an objection is raised.

If the trust uses IT systems to make automatic decisions based on personal data individuals have a right to object and:

- request human intervention in the decision making
- be able to express their point of view
- obtain an explanation of how a decision has been reached
- challenge the decision

This right does not exist if the automated decision making:

- is necessary to fulfil a contract to which they are party
- is authorised by law
- the data subject has consented to the processing

Individuals also have the right to object to data being used for research purposes unless the research is being undertaken in the wider public interest which outweighs a data subject's right to privacy.

Right to be Informed

The trust issues a privacy notice which explains what information the trust is processing, the legal basis for this, the purpose of processing, who the information is shared with and other information required by data protection legislation. The current privacy notice is available on the trust's website

13. Breaches of Data Protection

The trust has a data breach management process which all staff are aware of and have received appropriate training to help them recognise and react appropriately to data breaches. All breaches or suspected breaches of Data Protection legislation will be reported to the trust's Data Protection Officer who will ensure the process is adhered to and ensure breaches are reported to the ICO where necessary.

14. Information security

The trust's Information Security Policy covers the creation, acquisition, retention, transit, use, and disposal of all forms of information.

It applies to all employees and Trustees and Governors; it also applies to volunteers, work experience candidates, and all staff of service delivery partners and other organisations who handle information for which the trust is responsible. It will form the basis of contractual responsibilities in contracts with Data Processors where reference is made to the trust's Data Protection and Information Security Policy.

It is the policy of the trust that:

- we will protect information from a loss of:
  - confidentiality (ensuring that information is accessible only to authorised individuals)
  - integrity (safeguarding the accuracy and completeness of information)
  - availability (ensuring that authorised users have access to relevant information when required)
  - relevance (only keeping what we need for as long as it is needed)
- we will meet all regulatory and legislative information management requirements
- we will maintain business continuity plans
- we will deliver appropriate information security training to all staff
- we will make available appropriate and secure tools to all staff
- we will report and follow-up all breaches of information security, actual or suspected

Guidance and procedures will be maintained to support this policy. These will include procedural standards for individuals with access to information.

System operating procedures will be developed and maintained to ensure compliance with this policy.

Information systems are checked regularly for technical compliance with relevant security implementation standards.

Operational systems are subjected to technical examination to ensure that hardware and software controls have been correctly implemented.

15. Management of Information

The trust will manage information in accordance with the principles and procedures within this policy and other relevant policies and standards. The following principles apply to how we handle information in the trust:

- All identifiable personal information is treated as confidential and will be handled in accordance with the relevant legal and regulatory protocols.
- All identifiable information relating to staff is confidential except where national policy on accountability and openness requires otherwise.
- Procedures will be maintained to ensure compliance with Data Protection legislation, The Human Rights Act 1998, the common law duty of confidentiality, the Freedom of Information Act 2000 and any other relevant legislation or statutory obligation.
- Information is recorded, used and stored to protect integrity so that it remains accurate and relevant at all times.

16. Trust (Schools) records

We will create and maintain adequate pupil, staff and other records to meet the trust's business needs and to account fully and transparently for all actions and decisions. Such records can be used to provide credible and authoritative evidence where required; protect legal and other rights of the trust, its staff and those who have dealings with the trust; facilitate audit; and fulfil the trust's legal and statutory obligations.

Records will be managed and controlled effectively to fulfil legal, operational and information needs and obligations in the most cost-effective manner.

17. Contacts

Data Protection Officer

Peter Questier
East Sussex County Council, Information Governance Team
Schools.DPO@eastsussex.gov.uk

Office of the Information Commissioner

The Information Commissioners
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF
website: www.ico.gov.uk

Separated Parents Policy

Statement of intent

Cavendish Education Trust recognises that children from families whose parents are separated, or are undergoing separation, may go through traumatic changes during their time at school. With this in mind, we will make every effort to work with parents to promote the welfare of children.

This policy has been created to minimise any impact and to clarify to all parties what is expected from separated parents and what can be expected from the school and its staff.

1. Definitions

1.1. Schools have a legal duty to work in partnership with families and to involve all those with parental responsibility in their child's education. Section 576 of the Education Act 1996 defines a 'parent' as:

- All natural parents, whether they are married or not.
- Any person who, although not a natural parent, has parental responsibility for a child or young person.
- Any person who, although not a natural parent, has care of a child or young person (a person with whom the child lives and who looks after the child).

1.2. Parents as defined above must be treated equally, unless there is a court order limiting an individual's exercise of parental responsibility. In the event that the school is not informed of the existence of such an order, neither parent will have rights superior to the other.

1.3. Individuals who have parental responsibility, or care for a child, have the same rights as natural parents. This includes the right to:

- Receive information (e.g. pupil reports, school events etc.).
- Participate in activities (e.g. elections for parent governors).
- Give consent (e.g. for school trips).
- Be involved in meetings concerning the child (e.g. participate in an exclusion procedure, appeal against admission decisions).

2. Trust responsibilities

2.1. The Trust will ask parents or guardians for the names and addresses of all parents when they register a pupil.

2.2. It is the duty of the Trust to ensure that names and addresses of all parents, where known, are included in the admission register and also in pupil records, and are available to the pupil's teachers.

2.3. The Trust will ensure that names and addresses of all parents are forwarded to any school to which the pupil moves.

2.4. The Trust will ensure that details of court orders are noted in the pupil's record.

3. Parental Responsibilities

3.1. Parents are responsible for informing the Trust school when there is a change in family circumstances. We recognise the sensitivity of such situations and we will maintain confidentiality requested by parents as far as possible. The school will also not make judgements about individual circumstances, and both parents will be treated equally.

3.2. Where there is a court mandated restraining order in place, a copy needs to be retained by the school, which will put measures in place to ensure the child is not released to named individuals.

3.3. Parents who have joint custody of the child are requested to keep the school informed, in writing, of any disputes they have with each other regarding the collection of children.

3.4. Children's welfare and safety are paramount, where there are issues over access to children, the parent with whom the child resides should contact the school immediately.

3.5. The Trust schools' hold parents' evenings, where both parents are welcome and can make an appointment via the school office.

3.6. The schools' expects parents to communicate with each other regarding these arrangements.

3.7. Parents are expected to liaise and communicate directly with each other in matters such as the ordering of school photographs, tickets for performances and other instances. The school will not deal individually with these requests in view of the significantly increased workload that they represent.

4. Progress reports and pupil records

4.1. Any parent has the right to receive progress reports and review pupil records of their child.

4.2. If the parents are separated or divorced, progress reports will be sent to the parent and address noted in the school's records specifying where the child resides with the expectation that they will share the report with the other parent.

4.3. If the child is subject to a joint residence order and the school's records formally capture that the child resides at two addresses, then progress reports will be sent to both addresses.

4.4. The school will send copies of the progress reports to a parent with whom the child does not reside only if that parent submits a written request.

4.5. Disagreements between parents must be resolved between the parents and cannot be resolved by the school.

4.6. The school will maintain an open door policy with both parents and the class teacher will be available to discuss any issues.

4.7. In extreme circumstances, if there is a belief that a possible abduction of the child may occur or if the parent is disruptive, the police will be notified immediately.

5. Collecting a child from school

5.1. Where a separated parent has parental responsibility and requests to take the child during or at the end of the school day, the school will endeavour to ascertain that parents are in agreement, providing a non-contact order is not in place.

5.2. The Executive Headteacher Primary/Heads of School will use their discretion on the decision to allow a child to leave the premises with a non-resident parent in the Primary Phase.

6. Obtaining consent

6.1. If parental consent is required for outings or activities, the school will seek consent from the resident parent, unless the decision is likely to have a long-term and significant impact on the child or the non-resident parent has requested to be asked for consent in all such cases.

6.2. In cases where the school considers it necessary to seek consent from both parents, it is possible that one gives consent and the other withholds it. In such cases, the school will assume that parental consent has not been given.

7. Name changes

7.1. Parents are responsible for resolving potential conflicts about the change of a surname.

7.2. There must be consent from both parents after divorce or separation for registering a change of name of a pupil.

7.3. The school will ensure that the change in surname is supported by written evidence. The review of documentation and the final decision to authorize the name change will be made by the Designated Safeguarding Leads of the Trust.

7.4. A separated parent who has parental responsibility, but no longer lives with the child, may refuse to consent to changing the child's surname. In such cases, the parent wishing to change the child's name would need to apply to the courts for permission do so.

7.5. In circumstances where a name change has already been effected by the school and it is in the interest of the child, who might be known by a new name, to refer back to a different name, the school will make a decision holding the best interests of the child under paramount consideration.

Data in Transit Policy

This policy describes clear standards of practice to maintain good security when using, taking or sending sensitive or confidential trust data outside of their normally secure location.

Contents

Key points

- All employees and trustees/governors are personally responsible for taking reasonable and appropriate precautions to ensure that all sensitive and confidential data is protected.
- All sensitive and confidential electronic data being taken outside of its normally secure location must be encrypted.
- Data loss must be reported immediately to the Chief Executive Officer (CEO) / Chief Operating Officer (COO)
- Disciplinary action could be taken where employees do not follow the guidance set out in this policy.

1. Introduction

1.1 Sensitive and confidential data must be treated with appropriate security by all who handle them. 'Appropriate' is not defined in terms of hard and fast rules, but is meant to be a degree of precaution and security proportionate to the potential impact of accidental disclosure. It is not possible to set out precautions and actions to cope with all circumstances and conditions, therefore staff handling sensitive and confidential data MUST assume personal responsibility and make considered judgements in terms of how they handle data and if in any doubt, seek support from their Data Protection Officer (DPO).

1.2 Overall impact is determined by the degree of sensitivity of the data and the quantity involved, but we must remember that a single record about an individual can have a potentially massive impact on that individual if accidentally disclosed to others.

1.3 Consider: If you were working on very sensitive and private information about yourself, carrying it with you or sending it to someone - what would you do to protect it?

2. Purpose

2.1 This document is intended to prevent unauthorised disclosure of information by laying down clear standards of practice to maintain good security when using, taking or sending sensitive or confidential data outside of their normally secure location.

2.2 The need for this is driven by our duty to protect the information of individuals and the school. This duty arises from legislation relating to information security, the most notable of which is as follows;

- General Data Protection Regulation
- Data Protection Act 2018
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Human Rights Act 2000

3. Other Relevant Policies and Guidance

3.1 This policy does not stand alone, but should be read and acted upon in conjunction with the schools:

- Data Protection and Information Security Policy
- Acceptable Use Agreements
- Code of Conduct

4. Scope and who the policy applies to

4.1 The scope covers all circumstances where sensitive or confidential data are taken outside of their normally secure location. This includes data in all formats; non-electronic (paper) and electronic (e.g. on PCs, tablets, laptops and removable storage media).

4.2 Whilst the Policy refers to employees and trustees/governors, it also applies to temporary staff, volunteers, secondees, work experience candidates, and all staff of service delivery partners and other agencies that process our data.

5. Responsibilities

5.1 The trust maintains appropriate security and privacy of data that it uses to perform its functions and it will ensure that appropriate tools, training and guidance are available to staff and members i.e.:

- Secure network for storing and using electronic data
- Secure work locations for storing and using hard-copy data
- Encryption tools for transmission of data outside secure locations

5.2 Trust staff and trustees/governors will act in accordance with the following standards and guidance to ensure security and privacy of sensitive and confidential data outside of their normally secure location.

5.3 Organisations that use our data to help us deliver a service will have to confirm they comply with these or equivalent standards.

6. Disciplinary and other sanctions

6.1 The trust considers this policy to be extremely important.

6.2 Where trust employees or service delivery partners have acted in accordance with this standard, but a breach occurs through the action of others, they will be deemed to have acted reasonably.

6.3 However, if trust employees are found to be in breach of the policy and its guidance then they may be subject to disciplinary procedures up to and including dismissal.

7. ‘Common Sense’ Precautions

7.1 There are some 'common sense' precautions that you can take before sending or taking sensitive or confidential data outside of their normally secure location, these are:

- Check that you are not sending/taking more detail than is necessary i.e. will the information still meet the need if you remove the sensitive material or aggregate the data? (GDPR Principle: Data Minimisation)
- Check that the data you are sending/taking are correct and appropriate. (GDPR Principle: Data Accuracy)
- Check that you are sending the data to the correct person/address.
- Check how you intend to keep it secure. (GDPR Principle: Integrity and confidentiality)

8. Approved secure transfer mechanisms

8.1 Where possible always use a secure transfer mechanism. Examples of this are:

- Secure Email
- ESCC AnyComms (software that allows secure transfer of documents)

9. **Trust emails**

9.1 Emailing information between internal school mailboxes is secure. However, following best practice, you should always link or reference information rather than attaching a copy where possible.

9.2 If you are sending sensitive or confidential data by email to an external address (other than a secure address) you must make sure the recipient is correct, known and trustworthy

9.3 For emailing sensitive information to government bodies, use a GCSX/PSN service where available.

10. **Web Interface**

10.1 If you are transferring sensitive or confidential data through a web portal you must:

- Ensure that there is robust access control in place (i.e. unique username/password)
- Ensure that only the people who need the data can see them
- Ensure that the data are encrypted (https connection)

11. **Mobile Storage Devices**

11.1 If you are taking data with you on a Trust device, such as a tablet PC, laptop, digital camera, you must:

- Only use a trust approved device
- Do not take trust equipment outside of the UK without approval from Director of ICT

11.2 Take all reasonable precautions to keep the device and data safe and secure e.g.;

- Never leave it in plain sight in public places
- Never let others use your access or device.
- Never share your logins/passwords or must not keep them with the device
- Report loss/theft immediately
- If you take any trust IT devices home DO NOT leave it in your vehicle, always take all devices into the house. Devices should be put in the boot when driving not front or back seats where they can be seen

12. **Post**

12.1 The postal service is considered reasonably secure for small amounts or low impact data (i.e. records pertaining to an individual, but NOT including very sensitive personal data). As a minimum, there are precautions that you must take to prevent loss:

- Make sure that the recipient and destination address is correct, accurate and up-to-date
- Clearly mark the envelope/parcel with a return address in case of incorrect delivery
- Do not send the only copy of the data if it is practical to make and retain a duplicate. You must assess the impact of loss of the original and make a copy if that impact is unacceptable
- If you use a courier they must be known and trusted
- Consider using recorded/registered post when sending sensitive information
- Physical records must be sent in a suitable container i.e. robust and secure enough to prevent accidental loss and/or tampering

13. **Physical (Paper) records**

13.1 If you are taking sensitive or confidential information with you in non- electronic (paper) format you must:

- Make sure that there is no other option available to you
- Never take the only copy with you if it is practical to make and retain a duplicate. You must assess the impact of loss of the original and make a copy if that impact is unacceptable (where copies are made, ensure these are securely destroyed as soon as possible following their use).
- Take only as much as necessary and only for as long as necessary
- Transfer it back to its normally secure location as soon as reasonably possible

13.2 Take all reasonable precautions to keep the records safe and secure e.g.:

- Keep them with you whenever possible; lock them away securely when you can't
- Use a suitable container that prevents accidental loss and/or viewing by others
- Never leave them in plain sight in public places
- Report loss/theft immediately

14. **You must not!**

14.1 There are some data handling activities which are prohibited:

- Never share your network password with anyone.
- Storing sensitive or confidential data on any personal or non-trust equipment.
- Sending sensitive or confidential information as unsecured physical records.
- Leaving sensitive or confidential physical records in plain view of others (i.e. unattended in your office, on the back seat of your car, in a public place, on your kitchen table or even with you, but where they can be overlooked by others).
- Leaving any device holding sensitive or confidential information unattended in a non-secure environment.
- Leaving any device holding sensitive or confidential information in a vehicle overnight

15. **Reporting data loss**

15.1 Staff should report a loss of sensitive and/or confidential data to the Chief Executive Officer (CEO), Primary Executive Headteacher, Chief Operating Officer or PA to CEO and complete a data breach incident report form.

16. **Definitions**

16.1 Sensitive and confidential data

The following list is not exhaustive and contains examples of sensitive and confidential data:

- Any data that is marked Official Sensitive/Protect/Restricted
- Any data covered by the Data Protection Act - i.e. all data that relates to a living individual.
- Any data classified as Commercial in Confidence - e.g. data that relates to commercial proposals or current negotiations.
- Any data relating to security information, investigations and proceedings, information provided in confidence etc.
- An easy sense check on whether data is sensitive or confidential is to ask yourself:

- Is the data covered by the Data Protection Act 2018?
- Could release of the information cause problems or damage to individuals, the public, the trust, or, a partner organisation? This could be personal, financial, reputation or legal damage.
- Could release prejudice the outcome of negotiations or investigations?

16.2 Normally Secure Location

For the purposes of this policy standard 'normally secure location' is defined as:

- A secure storage facility with:
  - Access controls such as individual login accounts
  - Backup and recovery facilities
  - No public access
  - Anti-virus and firewall protection
- Secure buildings or parts of buildings with:
  - Physical access controls - swipe cards, keys etc.
  - No public access
  - Lockable storage facilities
  - Other protection systems e.g. alarms,

17. **Glossary**

Personal Data

Personal data is anything that relates to a living individual in which the individual can be identified directly from the information from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller.

Special Category Personal Data

Defined as being any personal data relating to racial or ethnic origin, political opinions, religious or similar beliefs, membership of a trade union, physical or mental health or condition, sexual life, the commission or alleged commission of any offence, any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

Special Category Data Policy

Summary
This policy outlines the trust's obligations under Data Protection Legislation with regard to the processing of Special Category Personal Data. This should be read alongside the trust's Data Protection and Information Security policy, and the privacy notice.

1. Policy Statement

Cavendish Education Trust is committed to ensuring that all personal data it processes is managed appropriately and in compliance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018) (collectively referred to as "DP legislation"). The trust recognises its duties to protect all personal data but in particular Special Category Personal Data as defined under Data Protection legislation i.e. information that may identify an individual's:

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade union membership,
- health,
- sex life/orientation
- genetic/biometric identifier
- criminal convictions/offences

The trust will ensure that all Special Category Data is captured, held and used in compliance with this policy. Any proposed new use of Special Category Data will be subject to a Data Protection Impact Assessment.

For all uses of Special Category Data, the processing will be included in the Record of Processing Activity (ROPA). This will include a description of the lawful basis for processing and confirmation that the appropriate data retention rules are being applied.

2. Responsibilities

The Chief Executive Officer (CEO) has overall responsibility for ensuring compliance with this policy and with Data Protection legislation across the trust.

The Data Protection Officer (DPO) has responsibility for advising the organisation on data protection matters, and for monitoring compliance with this policy.

All staff are responsible for understanding and complying with relevant policies and procedures for processing and protecting special category data.

3. Related Documents

- Data Protection Policy
- CCTV policy
- Record of Processing Activity
- Privacy notice

4. Compliance with the Principles

All processing of personal data, including Special Category Data, is subject to the

school's Data Protection and Information Security Policy and all related procedures for data handling.

Below is a summary of our procedures for compliance with the principles under Article 5 of GDPR.

Data Protection Principle	**Procedures for securing compliance**	**Relevant policies/ procedures**
Personal data will be processed lawfully, fairly and in a transparent manner	All use of Special Category Data will be: • Assessed for lawfulness, fairness and transparency as part of Data Protection Impact Assessments (DPIA) • described clearly and precisely in privacy notices available to data subjects The trust will ensure that personal data is only processed where a lawful basis applies, (i.e. is subject to clear justification under Article 6 and 9 of GDPR) The trust will only process personal data fairly, and will ensure that data subjects are not misled about the purposes of any processing	• Information Security/ Data Protection Policy • Privacy notices • ROPA • DPIA procedure / template • School data protection training document/log
Personal data will be collected and used for specified, explicit and legitimate purposes and not further processed in an incompatible way (*'purpose limitation'*)	This will be checked within the DPIA process. Staff will be trained to ensure that they do not use personal data for purposes other than those authorised by the organisation. Staff will receive training and document procedures for relevant processes. Data subjects will be informed of the purpose for processing in a privacy notice	• Data Protection Policy • Privacy notices • ROPA • DPIA procedure / template • Information governance or DP training for staff • School data protection training document/log
Personal data collected and processed will be adequate, relevant and limited to what is necessary for	To adhere to the principle of privacy by design, the school only collects and holds data as necessary for their operational requirements or to meet statutory obligations.	• Data Protection Policy • DPIA procedure / template • Information governance or DP training for staff • School data protection training document/log

the purpose for processing (*'data minimisation'*)	Staff have roles-based access and are trained to record only the minimal necessary personal data for business needs. This will also be checked within the school DPIA process.	
Personal data will be accurate and where required, rectified without delay (*'accuracy'*)	The trust has systems in place to verify the accuracy of the data it holds. These include; Data collection sheets Edulink	• Data Protection Policy • DP training for staff • School data protection training document/log
Personal data will not be kept in an identifiable form for longer than necessary (*'storage limitation'*) i.e. in line with the school retention schedule	The Chief Operating Officer in school has responsibility for ensuring that the retention schedule is applied to all personal data, and in particular to special category data. Where systems do not have the functionality to automate disposal, staff have a scheduled task to manually delete time-expired data.	• Data Protection Policy • Retention schedule • DP training for staff • School data protection training document/log
Personal data will be kept securely	All use of personal data is subject to our Data Protection and Information Security Policy and related security measures. Appropriate means of transmitting data are used. Data is securely stored and securely disposed of (where retention periods are reached). Where processing is sub-contracted or outsourced there are suitable Data Protection clauses in the contract.	• Data Protection Policy • Retention schedule • DP training for staff • School data protection training document/log

CCTV Policy (closed circuit television)

This policy relates to any Trust School operating CCTV

1 Introduction

1.1 The use of CCTV and images produced are for the following purposes;

- Safeguarding of staff, pupils and visitors
- Prevention or detection of crime such as protecting personal property of staff, pupils and visitors
- Ensuring the wellbeing of individuals on the trust sites
- Supporting the police in their duties, including identifying, apprehending and prosecuting offenders
- Protecting the trust buildings and assets

1.2 The CCTV system is owned and operated by Cavendish Education Trust, the deployment of which is determined by the Chief Executive Officer (CEO)/Primary Executive Headteacher (PEH).

1.3 The CCTV is monitored centrally from the IT and Site offices and Senior Leaders. Access to the images is controlled and approved by CEO/PEH.

1.4 The use of CCTV, and the associated images, are covered by the Data Protection Act 1998. This policy outlines the trust's use of CCTV and how it complies with the Act and the General Data Protection Regulation (GDPR).

1.5 Any changes to CCTV monitoring will be discussed between the CEO, PEH, Chief Operating Officer (COO) and the Director of ICT.

1.6 All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images. Through this policy, all operators are made aware of their responsibilities in following the CCTV Code of Practice. The trust's 'Data Controller' (CEO/PEH) will ensure that all employees are aware of the restrictions in relation to access to, and disclosure of, recorded images by publication of this policy.

2. Statement of Intent

2.1 The trust complies with the Information Commissioner's Office (ICO) CCTV Code of Practice to ensure that CCTV is used responsibly and safeguards both trust and confidence in its continued use. The Code of Practice is published at: https://ico.org.uk/media/1542/cctv-code-of-practice.pdf

2.2 CCTV warning signs are clearly and prominently placed at the main reception entrance to the school. Signs will contain details of the purpose for using CCTV (see appendix B).

2.3 The original planning, design and installation of CCTV equipment endeavoured to ensure that the scheme will deliver maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

3. Covert Monitoring

3.1 It is not the trust's policy to conduct 'Covert Monitoring' unless there are 'exceptional reasons' for doing so.

3.2 The trust may, in exceptional circumstances, determine a sound reason to set up covert monitoring.

For example:
a) Where there is good cause to suspect that an illegal or unauthorised action(s), is taking place, or where there are grounds to suspect serious misconduct.
b) Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

3.3 In these circumstances authorisation must be obtained from the CEO/PEH and advised before any commencement of such covert monitoring.

3.4 Cameras sited for the purpose of covert monitoring will not be used in areas which are reasonably expected to be private, for example toilet cubicles, changing areas etc.

4 Storage and Retention of CCTV images

4.1 Recorded data will be retained for 21 days. Extracts of recordings will be retained for no longer than is necessary.

4.2 All retained data will be stored securely at all times.

5 Access to CCTV images

5.1 Access to recorded images will be restricted to authorised staff to support the business of the Trust e.g. SLT, Site team, ICT team, Progress and Guidance. Access to recordings will not be made more widely available.

6 Subject Access Requests

6.1 Individuals have the right to request access to CCTV footage relating to themselves under the Data Protection Act and GDPR.

6.2 Any person wishing to exercise this right can do so by emailing or writing to the trust; office@cavendish.e-sussex.sch.uk. Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified. For example, date, time and location.

6.3 The trust will respond to requests within 1 month of receiving the request but if a request is received outside of the school term this may not be possible

6.4 The trust reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an ongoing investigation, or where another exemption applies under the Data Protection Act.

6.5 The trust will seek advice from its data protection officer (DPO) when dealing with SARs.

7 Access to and Disclosure of Images to Third Parties

7.1 There will be no disclosure of recorded data to third parties other than to authorised personnel such as the Police and service providers to the trust where these would reasonably need access to the data (e.g. investigators).

7.2 Requests for images/data should be made in writing to the CEO/PEH.

7.3 The data maybe used within the trust's discipline and grievance procedures as required, and will be subject to the usual confidentiality requirements of those procedures.

8 Complaints

8.1 Complaints and enquiries about the operation of CCTV within the trust should be directed to the CEO/PEH in the first instance.

Checklist

This CCTV system and the images produced by it are controlled by the Director of ICT who is responsible for how the system is used under direction from the trust's 'Data Controller'. Organisations using CCTV for the purposes of crime prevention need to pay a data protection fee to the Information Commissioner's Office (ICO), which the Trust pays annually as organisations that process personal data are required to pay the fee.

Cavendish Education Trust has considered the need for using CCTV and have decided it is required for the prevention and detection of crime and for protecting the safety of the trust schools'. (please see 1.1 above). It will not be used for other purposes. The trust will conduct regular reviews of our use of CCTV.

Checklist task	by
Annual data protection fee has been paid to the ICO	Chief Operating Officer
There is a named individual who is responsible for the operation of the system.	Director of ICT
A system had been chosen which produces clear images which the law enforcement bodies (usually the police) can use to investigate crime and these can easily be taken from the system when required.	Chief Operating Officer
Staff and members of the school will be consulted about any proposal to install / amend CCTV equipment or its use as appropriate.	Chief Operating Officer
Cameras have been sited so that they provide clear images.	Director of ICT
Cameras have been positioned to avoid capturing the images of persons not visiting the premises.	Director of ICT
There are visible signs showing that CCTV is in operation. Where it is not obvious who is responsible for the system contact details are displayed on the sign(s).	Director of Estates
Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them.	Director of ICT
The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated.	Chief Operating Officer / Director of ICT
Except for law enforcement bodies, images will not be provided to third parties.	Director of ICT
The organisation knows how to respond to individuals making requests for copies of their own images. If unsure, the data controller knows to seek advice from its Data Protection Officer.	Chief Operating Officer
Regular checks are carried out to ensure that the system is working properly and produces high quality images.	ICT Team

CCTV Signage
It is a requirement of the Data Protection Act 2018 to notify people entering a CCTV protected area that the area is monitored by CCTV and that pictures are recorded. The trust is to ensure that this requirement is fulfilled.

The CCTV sign should include the following:

- This area is covered by CCTV surveillance and pictures are recorded
- The purpose of using CCTV
- The telephone or contact address for any enquiries