

GDPR Policy

Item	Details
Policy Owner	Louise Morgan – CFOO
Review Level	Full Trustees
Approval Level	Full Trustees
Date Approved	22 September 2026
Effective Date	22 September 2026
Review Frequency	Annual
Next Review Date	21 September 2027
Version Number	1.1
Statutory / non-statutory	Statutory
Publication Location	Websites / Governance Management System / Internal

Checked By	Date
Executive Review	10/08/26
Legal / HR Review (where applicable)	10/08/26
Governance Review	22/09/26

Key roles

Data Protection Officer (DPO) of The Balcarras Trust:

Allocated from Gloucestershire County Council (GCC).

Data Protection Lead (DPL) of The Balcarras Trust:

Louise Morgan, Chief Operating Officer (CFOO) (LCM).

Contact details: trust@balcarras.gloucs.sch.uk

This policy applies to all academies and operations within The Balcarras Trust unless otherwise stated. It should be read in conjunction with the Trust's Scheme of Delegation and other related policies and procedures.

Contents

1. Aims	3
2. Legislation and Guidance	3
3. Definitions	3
4. The Data Controller	4
5. Roles and Responsibilities	4
5.1 The Trust	4
5.2 Data Protection Officer	4
5.3 Chief Executive Officer (CEO) and Chief Financial Operating Officer (CFOO)	5
5.4 All Staff	5
6. Data Protection Principles	5
7. Collecting Personal Data	6
7.1 Lawfulness, Fairness and Transparency	6
7.2 Limitation, Minimisation and Accuracy	6
8. Sharing Personal Data	6
9. Subject access requests and other rights of individuals	7
9.1 Subject access requests	7
9.2 Children and Subject Access Requests	8
9.3 Responding to Subject Access Requests	8
9.4 Other Data Protection Rights of the Individual	8
10. Parental Requests to see the Educational Record	9
11. Biometric Recognition Systems	9
12. CCTV	10
13. Photographs and Videos	10
14. Data Protection by Design and Default	10
15. Data Security and Storage of Records	11
16. Disposal of Records	12
17. Personal Data Breaches	12
18. Training	12
19. Monitoring arrangements	12
20. Related Policies and other documents	12
Appendix 1: Personal Data Breach Procedure	13
Appendix 2: CCTV Protocol	16

1. Aims

Our Trust aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data, regardless of its format.

2. Legislation and Guidance

This policy meets the requirements of the GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data. It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with our funding agreement and articles of association.

3. Definitions

Term Definition

Personal data

Any information relating to an identified, or identifiable, individual.

This may include the individual's:

- Name (including initials)
- Identification number
- Location data
- Online identifier, such as a username
- It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

Special categories of personal data

Personal data, which is more sensitive and so needs more protection, including information about an individual:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetics
- Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes
- Health – physical or mental
- Sex life or sexual orientation
- Processing

Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

Data subject

the identified or identifiable individual whose personal data is held or processed.

Data controller

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

Data processor

A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.

Personal data breach

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

4. The Data Controller

Each school in The Trust processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

Each school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and Responsibilities

This policy applies to all staff employed by The Trust, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 The Trust

The Trustees have overall responsibility for ensuring that our schools comply with all relevant data protection obligations.

5.2 Data Protection Officer

The Data Protection Officer (DPO) for The Balcarras Trust will be allocated by Gloucestershire County Council (GCC). Louise Morgan, CFOO is the Data Protection Lead (DPL) of The Balcarras Trust and is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

The DPL will provide an annual report of their activities directly to The Trustees within the CFOO Report and, where relevant, report to the board their advice and recommendations on Trust data protection issues.

The DPL is also the first point of contact for individuals whose data each school processes, and for the Information Commissioner's Office (ICO).

5.3 Chief Executive Officer (CEO) and Chief Financial Operating Officer (CFOO)

The CEO acts as the representative of the data controller on a day-to-day basis. The CEO delegates operational responsibility to a named Data Protection Lead (DPL) in each of the Trust's school. The CFOO will act as the Trust Data Protection Lead (DPL) and support the Data Protection Leads in each school with their roles and responsibilities.

The CFOO will ensure that data protection risks, compliance issues and significant incidents are transparently reported to Trustees in line with the accountability requirements set out in the Academy Trust Handbook 2026.

5.4 All Staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address

Contacting school's Data Protection Lead in the following circumstances:

- With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
- If they have any concerns that this policy is not being followed
- If they are unsure whether or not they have a lawful basis to use personal data in a particular way
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the
- European Economic Area (EEA)
- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

Contacting The Trust Data Protection Lead when their concern/query has not been effectively addressed by the School's Data Protection Lead.

6. Data Protection Principles

The GDPR is based on data protection principles with which The Trust must comply. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how The Balcarras Trust aims to comply with these principles.

7. Collecting Personal Data

7.1 Lawfulness, Fairness and Transparency

Each school only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task in the public interest, and carry out its official functions
- The data needs to be processed for the legitimate interests of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carers when appropriate in the case of a pupil) has freely given clear consent

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

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).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2 Limitation, Minimisation and Accuracy

We will only collect personal data for specified explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Gloucestershire County Council records retention schedule.

8. Sharing Personal Data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carers that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies.

When doing this, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us
- When appointing suppliers or contractors who process personal data, the Trust will comply with relevant DfE procurement frameworks and guidance. This includes ensuring that any supplier selected through a DfE-approved route meets required standards for data protection, security and value for money.
- Where personal data is processed in relation to severance payments, the Trust will ensure compliance with the Academy Trust Handbook 2026 requirements for approval and reporting. Any data shared with external bodies for this purpose will be limited, secure and lawful.

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.
- Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a ‘subject access request’ to gain access to personal information that The Trust holds about them.

This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn’t possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request, they must immediately forward it to The Trust's Data Protection Lead and The School's Data Protection Lead and await instruction.

9.2 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 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 a school in The Trust 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.

9.3 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

We will not disclose information if it:

- 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
- Is given to a court in proceedings concerning the child
- Any reference provided or received by a school in the Trust as part of an employment application or an application to move to another educational establishment. This is in line with the exemptions outlined in the 2018 Data Protection Act.
- If the request is unfounded or excessive, we may refuse to act on it or charge a reasonable fee which takes into account administrative costs.
- A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When we refuse a request, the Trust's DPL will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 Other Data Protection Rights of the Individual

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 (see section 7), 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
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Any individual wishing to exercise their data protection rights should submit their request to the Trust's Data Protection Lead (DPL). The DPL will coordinate the Trust's response and, where appropriate, seek advice and support from the Data Protection Officer (DPO).

Any member of staff who receives such a request must immediately forward it to their School Data Protection Lead or the Trust Data Protection Lead, as appropriate, to ensure the request is logged and managed within the statutory timescales.

10. Parental Requests to see the Educational Record

Parents of pupils in all schools in The Balcarras Trust have no statutory right of access to their child's educational record. However, we will endeavour to grant parents, or those with parental responsibility free access to their child's educational record (which includes most information about a pupil) within 30 school days of receipt of a written request.

11. Biometric Recognition Systems

Pupils' biometric data is used by some of the Trust Schools.

Where pupils' biometric data is used as part of an automated biometric recognition system (for example, pupils use fingerprints for payment system), the Trust will ensure that system fully complies with the requirements of the Protection of Freedoms Act 2012.

Parents/carers are notified about the biometric recognition system. The school gets written consent from at least one parent or carer before any biometric data is taken from their child.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). Alternative means of accessing the relevant services for those pupils are provided.

For example, pupils would be able pay for school dinners in cash at each transaction if they wished.

Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

12. CCTV

We use CCTV in various locations around The Trust's school sites 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 there are prominent signs in all of The Balcarras Trust schools making it clear CCTV is in use.

Any enquiries about the CCTV system should be directed to the School's Data Protection lead and/ or The Trust Data Protection Lead if relevant.

Please refer to Appendix 2 for further CCTV protocols including Dos and Don'ts (Page 16)

13. Photographs and Videos

As part of our Trust activities, we may take photographs and record images of individuals within any of our schools.

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/carers 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

Videos and photographs may be labelled with pupil's names or tutor groups when used in this way.

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.

14. Data Protection by Design and Default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified Trust DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge

- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matter; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:

For the benefit of data subjects, making available the name and contact details of each school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices) For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

Where financial information is published to meet the Academy Trust Handbook 2026 requirement to show how funding is distributed across schools, we will ensure that any personal data contained within such information is anonymised or removed in accordance with data protection law.

15. 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:

- The security of paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data will be carefully considered 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
- 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 governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our ICT acceptable use policy).
- 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 (see section 8)
- The Trust's approach to data security aligns with the DfE Digital and Technology Standards. We will continue to develop our systems and processes to meet these standards fully by 2030, ensuring secure, resilient and compliant digital infrastructure across all schools.
- Where Management Information Systems (MIS) process personal data on behalf of the Trust, procurement and contract renewal will comply with the DfE MIS Framework. This ensures that all MIS providers meet required standards for security, interoperability and data protection.

16. Disposal of Records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records and overwrite or delete electronic files. We may also use a third party to safely dispose of records on a Trust school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

17. Personal Data Breaches

The Trust will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

18. Training

All staff and governors 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.

19. Monitoring arrangements

The Balcarras Trust's DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated, if necessary, when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed every 2 years and shared with the full governing board.

20. Related Policies and other documents

This policy should be read in conjunction with other Trust policies and procedures, including those listed below. The list is not exhaustive and should be considered alongside any relevant statutory guidance.

- Freedom of Information Policy
- ICT Acceptable Use Policy

- AI Policy
- Complaints Policy
- Recruitment and Disclosure Policy
- Single Central Record Checklist
- Safeguarding Policy
- CCTV Policy (Appendix 2)

Appendix 1: Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify The Trust's Data Protection Lead. The Trust's DPL will feed back to School's Data Protection Lead on next steps.

The Data Protection Lead will investigate the report and determine whether a breach has occurred.

To decide, the data protection lead will consider whether personal data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been o Made available to unauthorised people

The Trust Data Protection Lead will alert the DPO. The CEO of The Trust will also be informed.

The DPO will work with The Trust's DPL and/ or The School's DPL to make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)

The DPO will work with The Trust's DPL and/ or The School's DPL to assess the potential consequences, based on how serious they are, and how likely they are to happen

The DPO will work with The Trust's DPL and/ or The School's DPL to work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

- Loss of control over their data
- Discrimination
- Identify theft or fraud
- Financial loss
- Unauthorised reversal of pseudonymisation (for example, key-coding)
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored within Trust SharePoint and/or the schools local drive, and/or GCC local drive depending on the level of investigation required.

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours.

As required, the DPO will set out:

- A description of the nature of the personal data breach including, where possible:
- the categories and approximate number of individuals concerned
- The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached.

This notification will set out:

- the name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

The DPO will document each breach, irrespective of whether it is reported to the ICO.

For each breach, this record will include the:

- Facts and cause
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored in the Trust section of the SharePoint.

The DPO and the CEO and The Trust's Data Protection Lead and if required The School's Data Protection Lead will meet to review what happened and how it can be stopped from happening again.

This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches:

We will take proactive measures such as those given below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

- Sensitive information being disclosed via email (including safeguarding records)
- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the schools data protection lead as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the school's data protection lead will ask the ICT department to recall it:
- In any cases where the recall is unsuccessful, the school's data protection lead will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The Trust's Data Protection Lead will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The Trust's Data Protection Lead will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Contents

1. Aims
2. Objectives
3. General Data Protection Regulations and CCTV Standards
4. Key Staff
5. Scope of Use
6. Code of Practice
7. Breaches of the Code
8. Disclosing CCTV Videos to Third Parties
9. Do
10. Don't

1. Aims

The purpose of this protocol is to regulate the management, operation and use of the CCTV system used by schools in The Balcarras Trust.

2. Objectives

- To increase personal safety of staff, students and visitors and reduce the fear of crime (safeguarding arrangements).
- To protect school buildings and their assets.
- To support the Police in a bid to deter and detect crime.
- To assist in identifying, apprehending and prosecuting offenders.
- To assist in the identification of pupils misbehaving around the school.
- To protect members of the public when on school premises.
- To assist in the prevention of damage and theft of private property.
- To assist in managing The Trust.

3. General Data Protection Regulations and CCTV Standards

Balcarras Trust has chosen to use CCTV (closed circuit television) in various areas across the schools including external entrances and identified areas within school buildings. The General Data Protection Regulations, Regulation of Investigatory Powers Act 2000 (RIPA) and CCTV Code of Practice issued by the Information Commissioner explains how CCTV systems should be used, so that schools and individuals can enjoy security and safety whilst ensuring that individual rights are upheld. Balcarras Trust complies with the code and adopts good standards of practice which helps towards realising this objective.

Use of CCTV can be affected by a number of Acts including the General Data Protection Regulations, the Human Rights Act and the Regulation of Investigatory Powers Act (RIPA).

4. Key Staff

Key staff have been provided with the necessary induction in the use of the CCTV systems and only those members of staff have access to the recordings within the system.

In each school, the staff provided with access to the CCTV will be:

The Site Manager
The Network Manager and members of the ICT Support Team
The Senior Leadership Team
The Pastoral Lead Team
The Duty Team Coordinators
The School Data Protection Lead
The Trust's Data Protection Lead
The Data Protection Officer

5. Scope of Use

The Balcarras Trust has undertaken the following checklist to ensure that the CCTV system remains within the law and that images can be used for prevention of rule breaking behaviour:

- The Trust has specified that the CCTV cameras have been installed for the safeguarding of staff and students and for detection and prevention of vandalism, rule breaking behaviour and crime prevention across The Trust estate.
- There are prominent signs in main reception (for all visitors to the school) and the pavilion entrance (for sports facilities users) making it clear CCTV is in use.
- Staff, pupils and parents are made aware that CCTV is used in the school via privacy notices published on each school website.
- The Trust retains the right to be the data controller for all footage recorded through the use of its CCTV cameras.
- The equipment is sited so that it only monitors those spaces that are intended to be covered by the equipment.
- All operators (staff who operate and monitor CCTV) are aware of the purposes for which the scheme has been established.
- Operators are aware that they are only able to use the equipment in order to achieve the purposes for which it has been installed i.e. safeguarding and the prevention and monitoring of misbehaviour.
- The images are stored on a secure server, and the retention period is for 90 days.
- In the event of behaviour events being reported footage may be reviewed and used by staff in resolving the situation.

6. Code of Practice

- This CCTV Protocol will be reviewed regularly.
- The CCTV system is owned and operated by The Trust.
- The footage may only be viewed by authorised members of staff as listed above.
- Images required as evidence will be removed from the server and stored in a secure location.

7. Breaches of the Code

Any breach of the code of Practice by The Trust will be initially investigated by the individual school's Data Protection Lead, in order for them to take the appropriate disciplinary action.

Any serious breach of the Code of Practice will be immediately investigated, and an independent investigation carried out to make recommendations on how to remedy the breach.

The following Dos and Don'ts as advised as part of the Data Protection Protocol and are adhered to by The Balcarras Trust and all schools within.

8. Disclosing CCTV Videos to Third Parties

The school will comply with all GDPR regulations when allowing third parties to view CCTV footage.

Where CCTV has been used to identify misbehaviour by a pupil, parents or carers of pupils will not be given permission to view the recorded videos.

9. Do

- ✓ Staff will record on CPOMS where CCTV has been used to identify misbehaviour.
- ✓ Formally assess the appropriateness of and reasons for, using CCTV.
- ✓ Undertake regular reviews of both the use of the CCTV system and the procedures to ensure compliance with the law.
- ✓ Ensure that film / images are not kept for longer than necessary – currently the data retention is for 90 days.
- ✓ Process (working with, using, passing on data) images in a lawful manner.
- ✓ Establish and document the person who is responsible for ensuring day-to-day compliance with the requirement of the CCTV Code of Practice.
- ✓ Make certain there are procedures for dealing with police enquiries, i.e. access under the GDPR or removal of evidence under Police and Criminal Evidence Act.
- ✓ Where footage is requested by a third-party, sufficient checks are made by verifying identities and having written proof (e.g. Police request) that the persons making the request, are authorised to do so. Detail should also be given how to identify the intended footage (e.g. time of day, what person was wearing etc).
- ✓ Export video or images and store them in secure locations on the network and that only the intended recipient(s) receive them.
- ✓ Access to CCTV recordings will be restricted to authorised individuals. Where necessary, footage may be shared with relevant staff, Trustees, or Local Governing Board (LGB) governors in consultation with the DSL and/or DPO, and only where such access is necessary, proportionate, and in accordance with data protection legislation.

10. Don't

- × Film areas that could amount to an infringement of personal privacy.
- × Ignore subject access requests (an individual's written request to access information about themselves under the General Data Protection Regulations). A person identifiable on CCTV images may be entitled to view the footage and may make a request to do so.
- × Use CCTV footage for any other purpose other than what it was originally used for e.g. Prevention and detection of a crime or detection of breaking school rules.
- × Use covert (i.e. where it is calculated to ensure that the persons are unaware) monitoring.
- × Use inadequate equipment. Blurred or indistinct images could constitute as inadequate data, whilst poorly maintained equipment may not provide legally sound evidence.
- × Disclose data to third parties, unless it is lawful to do so.
- × Systematically monitor people by use of CCTV.

11. Related Policies and other documents

This policy should be read in conjunction with other Trust policies and procedures, including those listed below. The list is not exhaustive and should be considered alongside any relevant statutory guidance.

- GDPR Policy
- Freedom of Information Policy
- ICT Acceptable Use Policy
- Safeguarding and Safer Working Protocol and Procedures Policy
- Complaints Policy
- Staff Code of Conduct
- AI Policy