St Joseph's College
Data Protection Policy

Date Reviewed -	**Autumn 2nd Half-Term 2023**
Next Review -	**Autumn 2nd Half-Term 2025**
Policy Author -	**Mr S Cabrera (Director of Development)**

Chair of Governor's signature: Mr S Horsman

To inspire the minds of all generations through education, with fearless faith.
As a united community we demonstrate our Lasallian values of faith, service, and respect.
Mission Statement

Contents

1. Aims....3
2. Legislation and guidance....3
3. Definitions....3
4. The Data Controller....4
5. Roles and Responsibilities....4
   5.1 Governing board....4
   5.2 Data protection officer....4
   5.3 Headteacher....4
   5.4 All staff....4
6. Data protection principles....5
7. Collecting personal data....5
   7.1 Lawfulness, fairness and transparency....5
   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....9
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....11
17. Personal data breaches....11
18. Training....12
19. Monitoring arrangements....12

Appendix 1: Personal data breach procedure....13

1. Aims

Our college 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 (EU) 2016/679 (GDPR) and the Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data, regardless of whether it is in paper or electronic 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.

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

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, living 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's: › 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

TERM	DEFINITION
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

Our college processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller. The college is registered with the ICO, as legally required.

5. Roles and Responsibilities

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

5.1 Governing board

The governing board has overall responsibility for ensuring that our college complies with all relevant data protection obligations.

5.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on college data protection issues.

The DPO is also the first point of contact for individuals whose data the college processes, and for the ICO.

Our DPO is Mr Stephen Cabrera and is contactable via scabrera@sjc.ac

5.3 Headteacher

The Headteacher acts as the representative of the data controller on a day-to-day basis.

5.4 All staff

Staff are responsible for:

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

- Contacting the DPO 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
    - If there has been a GDPR data breach by themselves s or someone within the organisation.
    - 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

6. Data protection principles

The GDPR is based on data protection principles that our college must comply with.

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 college aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will 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 college can fulfil a contract with the individual, or the individual has asked the college to take specific steps before entering into a contract.
- The data needs to be processed so that the college can comply with a legal obligation.
- The data needs to be processed to ensure the vital interests of the individual or another person i.e. to protect someone's life.
- The data needs to be processed so that the college, as a public authority, can perform a task in the public interest or exercise its official authority.
- The data needs to be processed for the legitimate interests of the college (where the processing is not for any tasks the college performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden.
- The individual (or their parent/carer 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 under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given explicit consent.
- The data needs to be processed to perform or exercise obligations or rights in relation to employment, social security or social protection law.
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent.
- The data has already been made manifestly public by the individual.
- The data needs to be processed for the establishment, exercise or defence of legal claims.
- The data needs to be processed for reasons of substantial public interest as defined in legislation.
- The data needs to be processed for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law.
- The data needs to be processed for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law.
- The data needs to be processed for archiving purposes, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest.

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given consent.
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent.
- The data has already been made manifestly public by the individual.
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights.
- The data needs to be processed for reasons of substantial public interest as defined in legislation.

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

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

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.

We will keep data accurate and, where necessary, up-to-date. Inaccurate data will be rectified or erased when appropriate.

In addition, 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 college's record retention schedule.

8. Sharing Personal Data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a pupil or parent/carer 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 contract with the supplier or contractor 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

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

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 internationally, 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 college 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
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- 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
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

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

If staff receive a subject access request in any form they must immediately forward it to the DPO.

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 our college 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 (or receipt of the additional information needed to confirm identity, where relevant)
- 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 may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

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 (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- 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)

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

10. Parental Requests to see the Educational Record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 college days of receipt of a written request.

If the request is for a copy of the educational record, the college may charge a fee to cover the cost of supplying it.

This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

11. Biometric recognition systems

Note that in the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18.

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive college dinners instead of paying with cash we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The college will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils can 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 college'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 college will delete any relevant data already captured.

12. CCTV

We use CCTV in various locations around the college site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV. See Appendix 2 for full CCTV policy.

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

Any enquiries about the CCTV system should be directed to the Helpdesk Team

13. Photographs and videos

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

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

Any photographs and videos taken by parents/carers at college events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.

Where the college takes photographs and videos, uses may include:

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

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

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

See our Child protection, safeguarding and Social Media policy for more information on our use of photographs and videos.

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 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 data protection impact assessments where the college'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 matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Appropriate safeguards being put in place if we transfer any personal data outside of the European Economic Area (EEA), where different data protection laws will apply
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our college 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, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the EEA and the safeguards for those, retention periods and how we are keeping the data secure.

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:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the college office
- Passwords that are at least 10 characters long containing letters and numbers are used to access college computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites
- 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 college-owned equipment
- 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)

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 the college'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 college 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.

All GDPR breaches are reported to our external monitoring support, GDPRIS, who will advise on appropriate courses of action for each breach..

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches in a college context may include, but are not limited to:

- A non-anonymised dataset being published on the college 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 college 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 college's processes make it necessary.

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed every **2 years** and shared with the full governing board.

Appendix 1: Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

All alleged data breaches will be recorded on the GDPRis platform on the College's breach and cyber log. GDPRis will provide support and guidance on appropriate next steps and this is recorded on the log ensuring that the College is compliant with GDPR procedures.

On finding or causing a breach, or potential breach, the staff member, governor or data processor must immediately notify the data protection officer (DPO) by email.

The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

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

Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation.

If a breach has occurred or it is considered that this is likely the case, the DPO will alert the Headteacher and if advised by the GDPR advisor the chair of governors.

The DPO will report any breach to GDPRis, GDPR in colleges, where it will be recorded on the College's Breach and Cyber log. GDPRis will advise the DPO on appropriate action to be taken in relation to the breach. In serious incidents this may mean that the incident must be reported to the ICO.

The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types at the end of this procedure)

The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen before and after the implementation of steps to mitigate the consequences

The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool

The DPO will document the decisions (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the college's awareness of the breach. 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 of the college's awareness of the breach. 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

Where the college is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:

- A description, in clear and plain language, of the nature of the personal data breach
- 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 consider, in light of the investigation and any engagement with affected individuals, whether to 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 electronically and manually

The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

The DPO and headteacher will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the college to reduce risks of future breaches

Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, 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.

Any breaches or alleged breaches are recorded on the GDPRis portal where they will be logged and reviewed by a GDPR expert.

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 DPO as soon as they become aware of the error.

If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the [ICT department/external IT support provider] to attempt to recall it from external recipients and remove it from the college's email system (retaining a copy if required as evidence).

In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether appropriate to 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 DPO will endeavour to obtain a written response from all the individuals who received the data, confirming that they have complied with this request.

The DPO 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

If safeguarding is compromised, the DPO will inform the designated safeguarding lead and discuss whether the college should inform any, or all, external safeguarding parties.

Other types of breach that you might want to consider could include:

- Details of pupil premium interventions for named children being published on the college website
- Non-anonymised pupil exam results or staff pay information being shared with governors
- A college laptop containing non-encrypted sensitive personal data being stolen or hacked
- The college's cashless payment provider being hacked and parents' financial details stolen
- Hardcopy report sent to the wrong pupil or families

Appendix 2: St Joseph's College CCTV Policy

1. Purpose

The purpose of this policy is to regulate the management, operation and use of the CCTV system (Closed Circuit Television)

CCTV systems are installed in premises for the purpose of enhancing security of the building and its associated equipment as well as creating a mindfulness among the occupants, at any one time, that a surveillance security system is in operation within and/or in the external environs of the premises during both the daylight and night hours each day.

CCTV surveillance at the college is intended for the purposes of:

- protecting the college buildings and college assets, both during and after college hours
- promoting the health and safety of staff, pupils and visitors as well as for monitoring student behaviour
- preventing bullying
- reducing the incidence of crime and anti-social behaviour (including theft and vandalism)
- supporting the police in a bid to deter and detect crime
- assisting in identifying, apprehending and prosecuting offenders
- ensuring that the college rules are respected so that the college can be properly managed.

The system does not have sound recording capability.

The CCTV system is owned and operated by the college, the deployment of which is determined by the college's leadership team.

The introduction of, or changes to, CCTV monitoring will be subject to consultation with staff and members of the college community.

The college's CCTV is registered with the Information Commissioner under the terms of the Data Protection Act 2018 and the General Data Protection Regulation (GDPR) 2016/679.

All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images. All operators are made aware of their responsibilities in following the CCTV Code of Practice. All employees are aware of the restrictions in relation to access to, and disclosure of recorded images.

2. Scope

This policy relates directly to the location and use of CCTV and the monitoring, recording and subsequent use of such recorded material. The college complies with the Information Commissioner's Office (ICO) CCTV Code of Practice to ensure it is used responsibly and safeguards both trust and confidence in its use.

CCTV warning signs will be clearly and prominently placed at the main external entrance to the college. Signs will contain details of the purpose for using CCTV.

In areas where CCTV is used, the college will ensure that there are prominent signs placed within the controlled area. The planning and design have endeavoured to ensure that the system will give maximum

effectiveness and efficiency, but it is not guaranteed that the system will cover or detect every single incident taking place in the areas of coverage.

CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with all existing policies and related legislation. Video monitoring of public areas for security purposes within college premises is limited to uses that do not violate the individual's reasonable expectation to privacy. Information obtained in violation of this policy may not be used in a disciplinary proceeding against an employee of the college or a student attending the college. All CCTV systems and associated equipment will be required to be compliant with this policy following its adoption by the college.

CCTV monitoring will never be used in any observing or monitoring a member of staff's performance.

Recognisable images captured by CCTV systems are 'personal data'. They are therefore subject to the provisions of the General Data Protection Regulation and Data Protection Act 2018.

3. Location of Cameras

The cameras are sited so that they only capture images relevant to the purposes for which they have been installed (as described above), and care will be taken to ensure that reasonable privacy expectations are not violated. The college will ensure that the location of equipment is carefully considered to ensure that the images captured comply with the legislation. The college will make every effort to position the cameras so that their coverage is restricted to the college premises, which includes both indoor and outdoor areas.

CCTV will NOT be used in classrooms but in limited areas within the college that have been identified by staff and pupils as not being easily monitored.

Members of staff will have access to details of where CCTV cameras are situated.

CCTV Video Monitoring and Recording of Public Areas may include the following:

- Protection of college buildings and property: The building's perimeter, entrances and exits, lobbies and corridors, special storage areas, cashier locations, receiving areas for goods/services
- Monitoring of Access Control Systems: Monitor and record restricted access areas at entrances to buildings and other areas
- Verification of Security Alarms: Intrusion alarms, exit door controls, external alarms
- Video Patrol of Public Areas: Parking areas, Main entrance/exit gates, Traffic Control
- Criminal Investigations (carried out by the police): Robbery, burglary and theft surveillance

4. Access to CCTV Images

Access to recorded images will be restricted to the staff authorised to view them and will not be made widely available. Supervising the access and maintenance of the CCTV System is the responsibility of the Headteacher. The Headteacher may delegate the administration of the CCTV System to another staff member. When CCTV recordings are being viewed, access will be limited to authorised individuals on a need-to-know basis.

5. Subject Access Requests (SAR)

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

All requests should be made in writing to the Data Protection Officer. Individuals submitting requests for access will be asked to provide sufficient information to enable footage relating to them to be identified. For example: time, date and location.

The applicant may view the CCTV footage if available.

The college will respond to requests within 30 days of receiving the request.

The college reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an on-going investigation.

6. Access and Disclosure of Images to Third Parties

There will be no disclosure of recorded data to third parties other than authorised personnel such as the Police.

If an order is granted by a Court for disclosure of CCTV images, then this should be complied with. However, very careful consideration must be given to exactly what the Court order requires. If there are any concerns as to disclosure, then the Data Protection Officer should be contacted in the first instance and appropriate legal advice may be required.

Requests for images should be made in writing to the Data Protection Officer.

7. Responsibilities

The Headteacher will:

- Oversee the use of CCTV systems that are implemented in accordance with this policy.
- Oversee and co-ordinate the use of CCTV monitoring for safety and security purposes within the college.
- Ensure that all existing CCTV monitoring systems will be evaluated for compliance with this policy.
- Ensure that the CCTV monitoring is consistent with the highest standards and protections.
- Review camera locations and be responsible for the release of any information or recorded CCTV materials stored in compliance with this policy.
- Maintain a record of access (e.g. an access log) to or the release of tapes or any material recorded or stored in the system.
- Ensure that monitoring recorded tapes are not duplicated for release.
- Ensure that the perimeter of view from fixed location cameras conforms to this policy both internally and externally.
- Give consideration to both students and staff feedback/complaints regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment.
- Ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within the college and be mindful that no such infringement is likely to take place.

- Ensure that external cameras are non-intrusive in terms of their positions and views of neighbouring residential housing and comply with the principle of “Reasonable Expectation of Privacy”
- Ensure that monitoring tapes are stored in a secure place with access by authorised personnel only
- Ensure that images recorded on tapes/DVDs/digital recordings are stored for a period not longer than 31 days and are then erased unless required as part of a criminal investigation or court proceedings (criminal or civil).
- Ensure that camera control is solely to monitor suspicious behaviour, criminal damage etc. and not to monitor individual characteristics.
- Ensure that camera control is not infringing an individual’s reasonable expectation of privacy in public areas.

8. Data Protection Impact Assessments and Privacy

CCTV has the potential to be privacy intrusive. The college will perform a Data Protection Impact Assessment when installing or moving CCTV cameras to consider the privacy issues involved with using new surveillance systems to ensure that the use is necessary and proportionate and address a pressing need identified.

Appendix 3: Cyber Security Protocol

Purpose

This cyber security protocol outlines the guidelines and provisions for protecting our college's data and technology infrastructure from a variety of threats.

Scope

This protocol applies to all staff, governors, contractors, volunteers, and anyone else who has access to our systems and hardware, whether permanent or temporary.

Confidential Data

Confidential data is any information that is private or sensitive, such as student/parent/carer data, financial data, and personal information. All staff are obliged to protect confidential data from unauthorized access, use, disclosure, modification, or destruction.

Threats

Cyber threats are constantly evolving, but some of the most common include:

- Malware: Malicious software, such as viruses, worms, and Trojan horses, can damage or disable computer systems and steal data.
- Ransomware: Ransomware is a type of malware that encrypts a victim's files and demands payment in exchange for the decryption key.
- Phishing: Phishing emails and text messages attempt to trick users into revealing sensitive information, such as passwords or credit card numbers.
- Hacking: Hackers try to gain unauthorized access to computer systems and networks to steal data, install malware, or disrupt operations.
- Data breaches: Data breaches occur when confidential data is accidentally or intentionally exposed to unauthorized individuals.

Steps to Cyber Security

All staff must take steps to protect our college's data and technology infrastructure from cyber threats. This includes:

- Protecting devices: All devices, including laptops, tablets, and smartphones, should be password protected and have up-to-date antivirus software installed.
- Using strong passwords: Passwords should be at least 8 characters long and include a mix of upper and lowercase letters, numbers, and symbols. They should also be unique and not easily guessed.
- Being careful with emails and text messages: Do not open attachments or click on links in emails from unknown senders. Be suspicious of emails that ask for personal information or that seem too good to be true.
- Reporting suspicious activity: If you see anything suspicious, such as a strange email, a pop-up message, or a file that you don't recognize, report it to your IT department immediately.

Cybersecurity Measures Currently in place at SJC

We have implemented a comprehensive cybersecurity strategy to protect our college's digital infrastructure and valuable data. This strategy includes multiple layers of protection, such as:

- Network Security: A Sophos XG Firewall monitors and blocks all incoming and outgoing traffic to protect our network from unauthorized access.
- Device Protection: Sophos Central Antivirus protects all our devices, both internal and external, from malware and ransomware.
- Email Security: LibraESVA Email Filter filters all incoming and outgoing emails to protect us from phishing attacks and malware.
- Content Filtering: Sophos Web Filter controls which websites students and staff can access to prevent exposure to inappropriate or harmful content.
- Internet Service Provider Protection: LGFL, our internet service provider, blocks certain attack vectors that hackers use.
- Application Control: Applocker prevents the execution of unauthorized and potentially harmful applications on all devices.
- Strong Password Policy: We require all users to use strong passwords and change them every 90 days.
- Multi-Factor Authentication (MFA): Soon, all users will be required to use MFA to log in to their accounts.
- Secure External Access: We provide a VPN connection for secure remote access to the college network.
- Data Backup and Recovery: We use the VEEAM Backup system to regularly back up all our data.

These measures help us to protect our college's digital assets from a wide range of cyber threats. We are committed to cybersecurity and will continue to adapt our strategies as the cyber threat landscape evolves.

Artificial Intelligence (AI)

The use of AI. has been blocked for students on devices that are connected to the college network.

Additional Measures

In addition to the steps listed above, staff should also:

- Be careful about what information you share on social media.
- Keep software up to date.
- Be aware of the college's social media and Acceptable Use of ICT policies.

When Working Remotely

Staff who work remotely must take additional precautions to protect the college's data and technology infrastructure. This includes:

- Using a secure internet connection.
- Using a VPN (virtual private network) to connect to the college network.
- Storing college data on encrypted devices.

- Being careful about what information you share on public networks.

Disciplinary Action

Staff who violate this cyber security protocol may be subject to disciplinary action, up to and including termination of employment.

Conclusion

The college is committed to protecting its data and technology infrastructure. All staff are expected to comply with this cyber security policy.