St Mary Magdalene C of E School
with
Christ Church C of E Primary School

CCTV SYSTEM POLICY AND CODE OF PRACTICE

This policy was:	Written in	January 2019
	Reviewed	November 2021
	Next review	January 2023

CONTENTS PAGE

.

Statement of Intent

Our Policy

We, the Koinonia Federation: St. Mary Magdalene C of E School, Woolwich, Peninsula campuses and Christ Church C of E school (hereinafter referred to as the "**School"**), believe that Closed Circuit Television ("**CCTV"**) and other surveillance systems have a legitimate role to play in helping to maintain a safe and secure environment for all our staff, students and visitors. However, we recognise that this may raise concerns about the effect on individuals and their privacy and as such this CCTV System Policy and Code of Practice ("**Policy"**) is intended to address such concerns.

Purpose

At St Mary Magdalene and Christ Church C of E Schools, we take our responsibility towards the safety of staff, students and visitors very seriously. To that end, we use CCTV (installed at the School premises) to:

- Monitor any instances of aggression or physical damage to our School and its members.
- Deter violent behaviour and damage to the School.
- Increase personal safety of staff, students and visitors alike.
- Reduce the fear of crime within the School.
- Protect the School premises and any School assets.
- Support the Police in a bid to deter and detect crime in order to reduce crime.
- Assist in the identifying and apprehension of offenders on the School property.
- Offer increased protection to members of the public and private property.

Cameras will be used to monitor activities within the School grounds, its car park, in the vicinity of the access gates and other public areas to:

- Identify aggressive/criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and well-being of the School's students and staff, together with its visitors.
- Taking action to prevent a crime.

At our Peninsula campus, approximately 90 cameras are located at various places on the School premises. 35 cameras are located at various places at our Woolwich campus and 11 cameras are located at our Christ Church campus. Images from the cameras are recorded and stored onto a hard drive located within the Premises office and within the main office at Christ Church School. All imagery is only available to selected senior School staff, as directed by the Executive Co-Headteachers and the Facilities Manager.

The purpose of this Policy is to manage and regulate the use of surveillance and CCTV systems at our School and ensure that:

- We comply with the requirements of the General Data Protection Regulation ("**GDPR"**), effective as of 25 May 2018.

GDPR

The following paragraphs give a brief outline of what is required by CCTV control rooms to comply with the said Act.

These standards must be met if the requirements of the Act are to be complied with. These are based on the Data Protection Principles that state that data must be:

- Fairly and lawfully processed
- Processed for limited purposes and not in any manner incompatible with those purposes
- Adequate, relevant and not excessive
- Accurate
- Not kept for longer than is necessary (30days)
  Processed in accordance with the individual's rights
- Secure
- Not transferred to countries without adequate protection
  Guidance on good practice
- The images, all information and recordings that are captured are useable as data for the purposes we require them for and/or which are protected by the GDPR.
- We reassure those persons whose images are being captured, that the images are being handled in accordance with data protection legislation

Restrictions

Under no circumstances will the surveillance and the CCTV cameras be present in any changing/toilet facilities within the School.

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Recordings will never be released to the media for purposes of entertainment.

Effectiveness of our systems

The planning and design have endeavoured to ensure that the surveillance and CCTV system will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident-taking place in the areas of coverage.

Warning signs, as required by the Code of Practice of the Information Commissioner have been placed at all access routes to areas covered by the School CCTV.

Ownership

The School owns the surveillance and/or CCTV system and all disks containing images.

The surveillance and/or CCTV system will be strictly controlled by authorised personnel only as specified by the Executive Co-Headteachers.

Note: CCTV is not monitored.

Key individuals

Sarah Kotb is the Data Protection Officer ("**DPO**").
Mrs Wainwright and Mrs Harrison are the Executive Co-Headteachers.
Mr Aaron Flanagan is the Facilities Manager and licenced CCTV operator.

Application

This Policy covers all employees, workers, contractors, agency workers, consultants, directors, members, governors, parents, past or present students and may also be relevant to visiting members of the public. This Policy is non-contractual and does not form part of the terms and conditions of any employment or other contract.

Signed: …… Date: ……

Definitions

For the purpose of this Policy and the GDPR, the following terms have the following meanings:

- **CCTV:** means fixed and domed cameras designed to capture and record images of individuals and property.
- **Data:** is information that is stored electronically or in certain paper-based filing systems and may include Personal Data. In respect of CCTV, this generally means video images. It may also include static pictures such as printed screen shots.
- **Data Controllers:** means the person or organisation that determines when, why and how to process Personal Data. We (the School) are the Data Controller of all Personal Data used for our own commercial and educational purposes.
- **Data Processors:** means the person or organisation that is not a Data User that processes Personal Data on our behalf and in accordance with our instructions (for example, a supplier which handles Personal Data on our behalf).
- **Data Users:** are those of our employees whose work involves processing Personal Data. This will include those whose duties are to operate CCTV cameras and other surveillance systems to record, monitor, store, retrieve and delete images. Data users must protect the data they handle in accordance with this Policy and the School's Data Protection Policy.
- **Data Subjects**: means a living, identified or identifiable individual about whom we hold Personal Data as a result of the operation of our CCTV (or other surveillance systems).
- **Personal Data:** means any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This will include video images of Data Subjects.

Legal Framework

Applicable legislation

This Policy (and the use of CCTV) has and will continue to have due regard to legislation in the United Kingdom including, but not limited to, the following:

- The Children Act 1989.

- The Children Act 2004.
- The School Standards and Framework Act 1998.
- The Freedom of information Act 2000 ("**FOA**").
- The Regulation of Investigatory Powers Act 2000.
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004.
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016).
- The Equality Act 2010.
- The Protection of Freedoms Act 2012.
- The General Data Protection Regulation 2018.
- Human Rights Act 1998

Applicable statutory/non-statutory guidance notes

This Policy has been created with regard to the following statutory and/or non-statutory guidance notes:

- Home Office (2013) The Surveillance Camera Code of Practice - https://www.gov.uk/government/publications/surveillance-camera-code-of-practice
- **ICO** (2017) Overview of the General Data Protection Regulation (GDPR) - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/
- ICO (2017) Guide to the General Data Protection Regulation - https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf
- ICO (2017) In the picture: A data protection code of practice for surveillance cameras and personal information - https://ico.org.uk/media/1542/cctv-code-of-practice.pdf

Other Federation policies

This Policy operates in conjunction with the following School policies:

- Data Protection Policy
- Management and Retention of Data Policy

Data Protection Principles

What the Federation will do to comply with legislation

The Federation is the data Controller. In order to comply with the requirements of the applicable legislations (listed above), the School as the Data Controller will ensure that Data from CCTV footage will be:

- Legally and fairly processed in a transparent manner.
- Collected for specified, explicit and legitimate purposes and ensuring that it is used accordingly.
- Processed for limited purposes and not in any manner incompatible with those purposes.

- Stored for longer periods, in so far as such Data is processed for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (subject to implementation of the technical and organisational measures required under the GDPR).
- Adequate, relevant and not excessive in relation to the reason for its collection.
- Not kept for longer than is necessary and will be erased ad rectified without delay (having due regard to the purpose for which such Data was processed).
- Processed in accordance with individuals' rights.
- Accurate and, where necessary, kept up-to-date.
- Secure (by way of protection against unauthorised or unlawful processing and against accidental loss, destruction or damage).

Protocols

The surveillance and/or CCTV system will be registered with the Information Commissioner's Office ("**ICO"**) in line with data protection legislation.

The surveillance and/or CCTV system is a closed digital system.

Warning signs have been placed throughout the School premises where the surveillance and/or CCTV system is active, as mandated by the ICO's Code of Practice.

The surveillance and/or CCTV system has been designed for maximum effectiveness and efficiency as much as can be afford from a school budget; however, the School cannot guarantee that every incident will be detected or covered and 'blind spots' may exist. There may be further investment in the future to cover more surveillance and/or CCTV of the school.

The surveillance and/or CCTV system will not be specifically aimed at individuals unless an immediate response to an incident is required.

The surveillance and/or CCTV system will not be specifically aimed at private vehicles or property outside the perimeter of the School.

CCTV footage is not to be viewed by only one member of staff. There should always be two staff members reviewing CCTV. This may be the data processor and a staff member who has authorisation to view the footage and completed the correct request form.

The Role of the Data Protection Officer

The DPO is crucial and their key duties will include the following:

- Dealing with freedom of information requests and subject access requests in line with the GDPR, including the FOA.
- Ensuring that all Data Controllers, Processors and Users at the School handle and process surveillance and CCTV footage in accordance with the GDPR.

- Ensuring that surveillance and CCTV footage is obtained in line with legal requirements.
- Ensuring consent is clear, positive and unambiguous.
- Ensuring that surveillance and CCTV footage is destroyed in line with legal requirements when it falls outside of its retention period.
- Keeping a comprehensive and accurate record of all data processing activities, including surveillance and CCTV footage, detailing the purpose of the activity and making these records public upon request, **see Appendix.**
- Informing Data Subjects of how their data captured in surveillance and CCTV footage will be used by the School, their rights for the data to be destroyed and the measures implemented by the School to protect individuals' personal information.
- Preparing reports and management information on the School's level of risk related to data protection and processing performance.
- Reporting to the highest management level of the School, e.g. the governing board.
- Abiding by confidentiality requirements in relation to the duties undertaken while in the role.

The role of the Executive Co-Headteachers

The role of the Executive Co-Headteachers includes:

- Meeting with the DPO to decide where CCTV is needed to justify its means.
- Conferring with the DPO with regard to the lawful processing of the surveillance and CCTV footage.
- Reviewing the CCTV System Policy and Code of Practice to ensure it is compliant with current legislation.
- Monitoring legislation to ensure the Federation is using surveillance fairly and lawfully.
- Communicating any changes to legislation with all members of staff.

Security

<u>Operation of the system</u>

The surveillance and/or CCTV system will be administered and managed by the Facilities Manager, in accordance with the principles and purpose expressed in the code.

The day-to-day management of the surveillance and/or CCTV system will be the responsibility of both the Executive Co-Headteachers and the Facilities Manager.

The surveillance and/or CCTV system will only be operated and controlled by approved staff as directed by the Executive Co-Headteachers and the Facilities Manager.

See Appendix E for a comprehensive list of names.

Control units

The Facilities Manager will check and confirm the efficiency of the surveillance and/or CCTV system daily and in particular that the equipment is properly recording and that cameras are functional.

Access to the CCTV control Units will be strictly limited to those staff as approved by the Executive Co-Headteachers or the Facilities Manager.

See Appendix E for a comprehensive list of names.

Visitors and other contractors wishing to view the control units will be subject to particular arrangement as outlined below:

- Control unit operators must satisfy themselves over the identity of any other visitors wishing to view the control cabinet and the purpose of the visit.
- Where any doubt exists, access will be refused.
- Details of all visits and visitors will be endorsed in the control unit file.
- The surveillance and/or CCTV system may generate a certain amount of interest. It is vital that operations are managed with the minimum of disruption. Casual visits will not be permitted.
- Visitors must first obtain permission from the Executive Co-Headteachers or Facilities Manager and must be accompanied throughout the visit.
- Any visit may be immediately curtailed if prevailing operational requirements make this necessary.
- A visitor's log will be maintained in the Facilities Manager's office in the control unit file. Full details of visitors including time/data of entry and exit will be recorded.
- The control units are located in the main office and the Premises office, which are only accessible to authorised personnel and are locked during out of hours.
- Other administrative functions will include maintaining hard disc space, filing and maintaining occurrence and system maintenance logs.
- Emergency procedures will be used in appropriate cases to call the Emergency Services.

Captured Imagery Procedures

Adherence to data protection legislation

The School understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles. The School will notify all students, staff and visitors of the purpose for collecting CCTV data via notice boards, letters and emails.

Key considerations

The surveillance and/or CCTV system will:

- Be designed to consider its effect on individuals and their privacy and Personal Data.

- Be transparent and include a contact point, the DPO, through which people can access information and submit complaints.
- Have clear responsibility and accountability procedures for images and information collected, held and used.
- Have defined policies and procedures in place that are communicated throughout the School.
- Restrict access to retained images and information with clear rules on who can gain access.
- Consider all operational, technical and competency standards, relevant to the surveillance and/or CCTV system and its purpose, and work to meet and maintain those standards in accordance with the law.
- Be subject to stringent security measures to safeguard against unauthorised access.
- Be regularly reviewed and audited to ensure that policies and standards are maintained.
- Only be used for the purposes for which it is intended, including supporting public safety, the protection of pupils, staff and volunteers, and law enforcement.
- Be accurate and well maintained to ensure information is up-to-date

Retention of imagery/Data

In order to maintain and preserve the integrity of the imagery used to record events from the hard drive and the facility to use them in any future proceedings, the following procedures for their use and retention must be strictly adhered to:

- Each storage device will be identified by a unique number.
- The Data processor shall register the date and time of the event and date of storage device manufacture.
- If several members of SLT need to review an incident, then the footage will be saved onto an encrypted USB and signed over to a nominated member of staff for no more than 48 hours. This will then be returned to a data processor who will erase the data. This will be logged. (see CCTV request form).
- If the data is required for evidential purposes for an external party then the encrypted USB must be sealed, witnessed, signed by the Executive Co-Headteachers as well as the data processor, dated and stored in a separate and secure evidence tape store. This would be in the fire proof, lockable cupboard in the School Office.
- If a storage device is not manufactured for the police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed, signed by the Executive Co-Headteachers, dated and returned to the evidence tape store.
- If the storage device is to be archived the reference must be noted.
- Imagery may be viewed by the Police for the prevention and detection of crime, authorised officers of the local County Council for supervisory purposes, authorised demonstration and training.
- A record will be maintained of the release of all storage device imagery given to the Police or other authorised applicants. A register will be available for this purpose.

- Viewing of storage device imagery by the Police must be recorded in writing and in the log book. Police will usually view the CCTV footage on the premises and this would not warrant any concerns for the data to be leaked.
- Should storage device imagery be required as evidence, a copy may be released to the Police under the procedures described in this Policy. storage device imagery will only be released to the Police on the clear understanding that the storage device remains the property of the School, and both the storage device and information contained on it are to be treated in accordance with this Policy.
- The School also retains the right to refuse permission for the Police to pass to any other person the storage device or any part of the information contained thereon. On occasions when a Court requires the release of an original tape this will be produced from the secure evidence storage device store, complete in its sealed bag.
- The Police may require the School to retain the stored STORAGE DEVICE imagery for possible use as evidence in the future. Such storage devices will be properly indexed and properly and securely stored until they are needed by the Police.
- Applications received from outside bodies (e.g. solicitors) to view or release tapes will be referred to the Executive Co-Headteachers. In these circumstances the storage device imagery will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a Court Order. A fee can be charged in such circumstances: £50 for subject access requests; a sum not exceeding the cost of materials in other cases.

Access

Under the GDPR, individuals (to whom "Personal Data" relate) have the right to obtain confirmation that their personal information is being processed, including those obtained by CCTV.

Subject access request

In relation to Subject Access Requests ("**SAR**"):

- Individuals have the right to submit a SAR to gain access to their Personal Data in order to verify the lawfulness of the processing.
- SAR should be made on an application form available from the Executive Co-Headteachers and Facilities Manager.
- The School will verify the identity of the person making the request before any information is supplied.
- A copy of the information will be supplied to the individual free of charge; however, the School may impose a 'reasonable fee' to comply with requests for further copies of the same information.
- Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.
- Requests by persons outside the School for viewing or copying disks, or obtaining digital recordings, will be assessed by the Executive Co-Headteachers, who will

consult with the DPO, on a case-by-case basis with close regard to data protection and freedom of information legislation.

- Where a request is manifestly unfounded, excessive or repetitive, the School holds the right to refuse to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the ICO and to a judicial remedy, within one month of the refusal. Alternatively, the School may charge a reasonable fee if the request is accepted by the School.
- All fees will be based on the administrative cost of providing the information.
- All requests will be responded to without delay and at the latest, within one month of receipt.
- In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.
- In the event that a large quantity of information is being processed about an individual, the School will ask the individual to specify the information the request is in relation to.
- It is important that access to, and disclosure of, the images recorded by surveillance and CCTV footage is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact, should the images be required for evidential purposes.
- Releasing the recorded images to third parties will be permitted only in the following limited and prescribed circumstances, and to the extent required or permitted by law:
    - The Police – where the images recorded would assist in a specific criminal inquiry.
    - Prosecution agencies – such as the Crown Prosecution Service (CPS).
    - Relevant legal representatives – such as solicitors and barristers.
    - Persons who have been recorded and whose images have been retained where disclosure is required by virtue of data protection legislation and the FOA.

Requests for access or disclosure will be recorded and the Executive Co-Headteachers together with the DPO will make the final decision as to whether recorded images may be released to persons other than the Police.

See Appendix D for a copy of SAR form

Breaches of the code (including breaches of security)

Any breach of this Policy by the Federation staff will be initially investigated by the Executive Co-Headteachers with the assistance of the DPO, in order for him/her to take the appropriate disciplinary action.

Any serious breach of this Policy will be immediately investigated and an independent investigation carried out to make recommendations on how to remedy the breach. Following investigation, a breach of this Policy may be regarded as misconduct leading to disciplinary action, up to and including dismissal.

Assessment of the Policy

Performance monitoring, including random operating checks, may be carried out by the Facilities Manager and Data Protection Officer to ensure compliance with this Policy.

Complaints

Any complaints about the School's CCTV system should be addressed to the Executive Co-Headteachers.

Monitoring and review

This Policy will be monitored and reviewed on two-year basis by the DPO and the Executive Co-Headteachers to ensure that it meets legal requirements, relevant guidance published by the ICO and industry standards.

We may amend this Policy (at any time). The Executive Co-Headteachers will communicate changes to this Policy to all members of staff.

The scheduled review date for this Policy is **January 2023**.

Public information

Copies of this Policy will be available to the public from the Administration office and the Federation website.

Summary of Key Points:

- This Policy will be reviewed every two years.
- The CCTV system is owned and operated by the School.
- The Control unit is not open to visitors except by prior arrangement and good reason.
- Liaison meetings may be held with the Police and other bodies.
- Recording hard drives and compact discs will be used properly indexed, stored and destroyed after appropriate use.
- Tapes may only be viewed by authorised school officers, control unit staff and the Police.
- Storage device imagery required as evidence will be properly recorded witnessed and packaged before copies are released to the police.
- Any breaches of this Policy will be investigated by the Executive Co-Headteachers. An independent investigation will be carried out for serious breaches.
- Breaches of the Policy and remedies will be reported to the Executive Co-Headteachers.

Appendix A- CCTV locations

Peninsula Campus: Approximately 90 cameras located internally and external across the school site.

Woolwich Campus: Approximately 35 cameras located internally and external across the school site.

Christ Church Campus: 11 cameras located internally and external across the school site.

Appendix B – Checklist

This CCTV system and the images produced by it are controlled by the Facilities Manager. The school notifies the Information Commissioner about the CCTV system, including any modifications of use and/or its purpose (which is a legal requirement of the GDPR).

The School has considered the need for using CCTV and have decided it is required for the prevention and detection of crime and for protecting the safety of the school's community. It will not be used for other purposes. The school will conduct regular reviews of our use of CCTV.

CCTV Review actions	**Checked (Date if appropriate)**	**By**	**Date of next review**
Notification has been submitted to the Information Commissioner and the next renewal date recorded.	December 2020	DPO	08 October 2021
There is a named individual who is responsible for the operation of the system.	December 2020	Facilities Manager	February 2022
Staff and members of the school community will be consulted about any proposal to install/amend CCTV equipment or its use as appropriate.	December 2020	Executive Co-Headteachers	February 2022
Cameras have been sited so that they provide clear images.	December 2020	Facilities Manager	February 2022
Cameras have been positioned to avoid capturing the images of persons not visiting the premises. **Note: Woolwich- camera in carpark has a view of the street. Pen- cameras may capture passers-by.**	December 2020	Facilities Manager	February 2022
There are visible signs showing that CCTV is in operation. Where it is not obvious who is responsible for the system contact details are displayed on the sign(s).	December 2020	Facilities Manager	February 2022

Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them.	December 2020	Facilities Manager and Executive Co-Headteachers	February 2022
The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated.	December 2020	Facilities Manager	February 2022
Except for law enforcement bodies, images will not be provided to third parties, unless requested by an individual as a subject access request.	December 2020	Facilities Manager	February 2022
The Federation knows how to respond to individuals making requests for copies of their own images.	December 2020	Facilities Manager	February 2022
Regular checks are carried out to ensure that the system is working properly and produces high quality images.	December 2020	Facilities Manager	February 2022

Appendix C – CCTV Signage

It is a requirement of the GDPR to notify people entering a CCTV protected area that the area is monitored by CCTV and that pictures are recorded. The school is to ensure that this requirement is fulfilled.

The CCTV sign should include the following:

- That the area is covered by CCTV surveillance and pictures are recorded
- The purpose of using CCTV
- The name of the school
- The contact telephone number or address for any enquiries

Example sign

Appendix D – Subject Access Request Form

St Mary Magdalene C of E School
with
Christ Church C of E Primary School

General Data Protection Regulation Subject Access Requests in Schools

People have several rights under the General Data Protection Regulation, one of which is the right to access their personal data held by an organisation. This is known as a Subject Access Request.

The request
Applicants must put their request in writing asking for the information they want. Identification should be provided in order to satisfy the school of the applicant's identity (where required).

What information are they entitled to?
Individuals (members of the public and staff) are entitled to a copy of any information the school holds about them, where they are the focus of the information and the information says something significant about them. This type of information is known as 'personal data'.

If a school has engaged with a Local Authority e.g. for pension services and the applicant has requested this kind of information, the school must contact the service providers who may hold the information on their behalf, and request a copy of it. This is to ensure that the School meets its obligation to collate all information held, relating to the individual making the request.

Parents requesting information about their child
Parents do not have an automatic right to see information held about their child (other than educational records, requested under the Education (Pupil Information) (England) Regulations 2005). If a child is over 12 years old and is considered by the school to be mature, the child should be asked to request the information themselves. Alternatively, the parent can provide the school with written permission from their child, to release the child's records to them.

Schools should also consider the legal entitlement and appropriateness of the parent to receive the information, for example in cases where a parent does not have parental responsibility for the child. Where necessary legal advice should be sought.

Time scales
If the information requested forms part of an educational record, the school must make their disclosure within 15 working days. For all other types of information, the school must make their disclosure as quickly as possible and in any case within 40 calendar days.

Can I charge for this information?

Under the Subject Access Fee Regulations 2000 there is a fee that may be charged by the School if the request for information is manifestly excessive or unfounded, particularly if the request is repetitive. The fee charged will be determined on the basis of the administrative costs of complying with the request and therefore the level of the fee will vary depending on the remit of the request and the administrative costs incurred. The School will need to provide evidence to the requestor on how the request for information is manifestly excessive or unfounded.

Consult authors
If the school is in possession of any letters, emails, documents, handwritten notes etc. which have been written by staff, members of the public or other organisations, the school must contact the authors and consult with them over the release of this information. There are some occasions when an unreasonable refusal of consent to release the information, may be overridden. In determining whether it is reasonable to disclose a document without consent from the author, the school should consider the following:

- Is there a duty of confidentiality owed to the individual (i.e. the author)?
- What steps have been taken with a view to seeking consent?
- Is the author capable of giving consent?
- Has the author refused consent and if so, is it reasonable to override the refusal?

Are there any exemptions?
Yes. A list of the main exemptions can be found in Appendix one. Please note the list is not exhaustive.

How do I redact/obscure information?
Any information which you are applying an exemption to e.g. third-party data, must be completely obscured. One way of doing this is to cover the unwanted text with a black marker pen (do this on a copy not the original document). You will then need to photocopy this copy and check that you cannot see the text through the black. If necessary, repeat the process again.

If an exemption has been applied and text has been removed from a document, to the extent that the remaining text does not make sense, it may be appropriate to withhold the entire document.

Do I need to keep a copy of the information I disclose?
Yes, it is good practice to keep an accurate copy of the information disclosed, for two years in case the contents are disputed.

Criminal offence
It is a criminal offence to deliberately withhold (without lawful justification) or destroy personal data, when a Subject Access request has been made.

Contact
For any further question relating to making your subject access request and the information held please contact the school office, for any GDPR related questions please contact the schools Data Protection Officer on SKotb@koinoniafederation.com.

General Data Protection Regulation
Exemptions from Subject Access

Exemption	Summary
Prevention or detection of crime or the apprehension or prosecution of offenders, or assessment or collection of any tax or duty	This can only be applied if there is a real likelihood that the disclosure would prejudice those purposes.
Disclosure would result in serious harm to the physical or mental health or condition of the individual or some other person	This can only be applied where a 'health professional' has made this prognosis and there needs to be a real likelihood that the disclosure would cause serious harm to the individual. This applies to information held for education welfare, social work and health purposes only.
Third Party Data / Information about 'other individuals'	Data subjects are only entitled to information held about them. Schools are not obliged to comply with a request if it would identify someone else, unless the other individual has consented to the disclosure of the information, or it is reasonable in all the circumstances to comply with the request without the consent of the other individual.
Legal Professional Privilege	This relates to the confidentiality between a client and their legal adviser. Any advice which comes from a legal advisor may be exempt from disclosure and should not be disclosed without the legal advisor's permission.
Confidential references given by the data controller	Schools are not obliged to disclose references which they have provided. However, they are obliged to disclose references which they have received. Any information which would identify the referee must be removed unless the referee consents to the release their information.
Cost of complying exceeds the appropriate limit	Unstructured, paper held documents and records are exempt from disclosure if it would take longer than 18hrs to locate and extract the information the data subject is entitled to, from within those documents and records. This exemption cannot be applied to educational records, social services records, health records or any other information held electronically.
Self-incrimination	If by complying with any subject access request the school would reveal evidence of the commission of any offence, other than an offence under GDPR, exposing them to proceedings for that offence, the school need not comply with the subject access request.
Prohibited or restricted by law	Where an act of law or an order from a court prohibits the disclosure.
Negotiations	

	Where the information contains the intentions of the school in relation to any negotiations with the data subject, that information is exempt from disclosure, if disclosure would prejudice those negotiations.
Examination Scripts	Information recorded by candidates during an examination is exempt from disclosure. However, any comments recorded by the examiner in the margins of the script are not exempt and as such should be provided even though they may not appear to the school to be of much value without the script itself.
Examination Marks	This is not an exemption as such but is rather an adaptation of the requirement to disclose personal data within 40 calendar days. If a Subject Access request is received for examination marks, the school can extend the 40-day timescale to be either 5 months from the day on which the school received the request or 40 calendar days from the announcement of the examination results, whichever is earlier.

This is not an exhaustive list

SUBJECT ACCESS REQUEST FORM

Dear school,

Please provide me with the information about me that I am entitled to under the General Data Protection Regulation. This is so I can be aware of the information you are processing about me, and verify the lawfulness of the processing.

Here is the necessary information:

1. Details of applicant/representative:	
Full name	
Date of request	
Name of school including campus (e.g. Peninsula, Christ Church, Woolwich)	
Relationship with the school	Please select: Pupil / parent / employee / governor / volunteer Other (please specify):
Correspondence home address	
Contact number	
Email address	
Details of the information requested	Please provide me with: Insert details of the information you want that will help us to locate the specific information. Please be as precise as possible, for example: I wish to view the CCTV of the X incident on X date at X time
Are you the data subject? (The persons whose information is being requested)	**Yes** **No** (If you are requesting information/records on behalf of a pupil please complete section 2)
Details for Identity Verification	I understand that I must be able to verify my identity. I will provide upon request x2 forms of identification from the list below to enable my request to be processed. Passport UK Driving License Birth Certificate Utility Bill

1. Details of applicant/representative:	
	Other (please specify)

2. Requests made on behalf of a pupil	
Full name of child	
Name of school including campus (e.g. Peninsula, Christ Church, Woolwich)	
Class (if a current pupil)	
Date of leaving (if applicable)	
Home address	
Contact number	
Email address	
Are you acting on behalf of the data subject with their written consent or in another legal authority?	**Yes** **No**
If 'Yes' please state your relationship with the data subject (e.g. parent, legal guardian or solicitor)	
Has proof been provided to confirm you are legally authorised to obtain the information? (E.g. letter of authority, this is required where the child is over 12 years of age|	**Yes** **No**
Please state in detail which information/records you require	

FOR OFFICE USE			
Receipt Date:		Reference no:	
ID required/received:		Received by:	
Proof of address required/received:		Fee required/received:	

Appendix E- Authorised CCTV Personnel

Campus	Position	Name	Authorisation level
Federation staff	Facilities Manager	Aaron Flanagan	Authorised to show and sign off request to see CCTV
	Executive Co-Headteacher	Claire Harrison	Authorised to sign off request to see CCTV
	Executive Co-Headteacher	Victoria Wainwright	Authorised to sign off request to see CCTV
PEN Secondary	Principal	Raz Hussain	Authorised to sign off request to see CCTV
	Vice Principal	Tom Greenwood	Authorised to sign off request to see CCTV
	Vice Principal	Zoe Pett	Authorised to sign off request to see CCTV
	Head of 6th form	Natasha Kwabi	Authorised to sign off request to see CCTV
	Assistant Principal	Sophie Alderson	Authorised to sign off request to see CCTV
	Assistant Principal	Monica Brady	Authorised to sign off request to see CCTV
	Assistant Principal	Julian Golding	Authorised to sign off request to see CCTV
Federation	IT Manager	Steve Khiogo	Authorised to show CCTV
PEN	Premises assistants	Lindo Covington/Dave Croucher	Authorised to show CCTV
PEN Primary	Deputy Headteacher	Dayo Ajayi	Authorised to sign off request to see CCTV
	Senior Assistant Headteacher	Kyla Butterworth	Authorised to sign off request to see CCTV
Christ Church	Deputy teacher	Sam Reid	Authorised to sign off request to see CCTV
	Senior Assistant Headteacher	Alex Ermellino	Authorised to sign off request to see CCTV
	Premises officer	Graham Cook	Authorised to show CCTV
Woolwich	Head of school	Tiffany King	Authorised to sign off request to see CCTV
	Senior Assistant Headteacher	Sarah Ringmo	Authorised to sign off request to see CCTV
	Premises officer	Simon Lockwood	Authorised to show CCTV

Appendix F- CCTV Footage Request Form

You must have a specific purpose for requesting to view CCTV as stated in the policy e.g. to investigate how property has been damaged or to investigate a report of physical violence etc.

This form MUST be completed either electronically or by hand when requesting to view CCTV footage.

Section 1 is to be completed by the requester and is be to be signed by an Authorised CCTV Personnel (see table)

Urgency guidelines for request form

L= low – CCTV will be reviewed within 24 hours

M = medium – CCTV will be reviewed after school/when the authorised person has completed the task they were carrying out

H = high – CCTV will be reviewed within the hour of receiving the request

Name of requestor	Date and urgency (L/M/H) of request	Description of incident	Number of people involved	Any further action required (if yes please state)

Only Authorised CCTV Personnel should sign this section

Signed by	Print name	Date

Section 2 is to be completed by the CCTV user who is showing the CCTV footage to the requester.

Campus	Position	Name
Federation staff	Facilities Manager	Aaron Flanagan
	IT Network Manager	Steve Khiogo
PEN	Premises staff	Dave Croucher/Arlindo Covington
Christ Church	Premises staff	Graham Cook
Woolwich	Premises staff	Simon Lockwood

CCTV operator name	Date footage was shown	Request for footage to be put on storage device (e.g. on an encrypted USB)	If yes please state why and how long it will be kept for	Log ID reference number of storage device (Ref number that matches the storage device e.g. USB)	How will the storage device be kept (e.g. will the USB be stored in a locked safe)

Only authorised staff should sign this section

Signed by	Print name	Date

Please retain the original copy of this request in the premises office in the CCTV request folder.

Unique number on the USB device		
Date, time and name of person USB is given to		
What data is held (incident):		
Date to be returned:		
Sign off date data is erased:	**time:**	**signature:**

: