Introduction

This policy sits below George Watson's College **Information Security - Overarching Policy**.

For George Watson's College ("the School"), Closed Circuit Television 'CCTV' surveillance systems have a legitimate role to play in helping to maintain a safe and secure environment for all of its pupils, staff and visitors. The School accepts that this may raise concerns about the effect on individuals and their privacy.

CCTV and its use is governed by the *Data Protection Act 2018 (DPA)* and the *General Data Protection Regulation 2016/679 (GDPR)*. This policy ensures CCTV on the School's estate is controlled appropriately to facilitate the School's legal obligations, best practice and to reduce risk of data loss.

In accordance with *General Data Protection Regulation 2016/679 (GDPR)* the School has registered its use of CCTV with the Information Commissioner.

This CCTV Policy must be read in conjunction with the School's Privacy Policies, available on the School's website.

1. Purpose

This policy sets out how the School operates and manages CCTV. It ensures that access to the School's CCTV systems is restricted to authorised personnel and the systems are used for lawful purposes, whilst helping to maintain a safe and secure environment for staff, pupils and visitors.

This policy is intended to replace any guidelines already in place within the School that relate to the physical operation and use of the CCTV system.

This policy must be read by any person/employee/contractor who will process personal data belonging to the Data Controller, (the School).

2. Scope

This CCTV Policy applies to all CCTV cameras and systems and any individual(s) accessing, viewing, disclosing or requesting access to the Schools CCTV systems.

3. Policy Statement

3.1 Why Does the School Use CCTV?

The School uses CCTV for the purpose of a public task duty; the management and security of the campus, monitoring health and safety and safeguarding of the pupils, parents, visitors and employees on campus.

By using CCTV, the School can monitor occurrences on campus and also the security of the buildings and grounds.

The School uses CCTV for the purposes of preventing, detecting or investigating crime and discloses images to law enforcement agencies.

The footage may also be used to investigate any alleged disciplinary issue, complaints raised or assist in managing the School in the event of serious incidents.

3.2 How the School Uses CCTV

3.2.1 Installation and Maintenance

The procedures appended to this policy will be followed in order to ensure that the School complies with legislation and Information Commissioner's Office CCTV Code of Practice.

When installing CCTV several components will be taken into consideration, such as:

- Careful consideration on the position of the cameras
- Cameras are not hidden from view and are sited in such a way as to ensure that they only monitor spaces intended to be covered
- Signs are displayed so that everyone is aware that they are entering a premises that is covered by surveillance equipment
- Signs indicate the purposes for which cameras are installed
- Trained and authorised personnel in the management and operations of the CCTV System
- The CCTV system is accessed from a secure area and controlled by the CCTV managers and operators
- A clear procedure exists for requesting, viewing, accessing and disclosing CCTV, and a record kept of all requests
- Maintenance of the CCTV system is carried out by a party approved by the CCTV manager.

Any changes to CCTV monitoring will be subject to a Data Protection Impact Assessment (DPIA) for which the School's Bursar will provide advice.

3.2.3 Audio Recordings

Although most CCTV cameras are capable of recording sound, this functionality is switched off by default, meaning there is no sound recorded throughout the campus. In the exceptional circumstances where audio recording is justified and this must be agreed in advance with the Bursar, it must be limited to that which is necessary to achieve the purposes specified.

Appropriate signage and notification must make it clear that audio recording is or may be carried out.

3.2.4 Records

A record of access and disclosure will be kept for disclosure of images in accordance with clause 3.5 and Annex A - CCTV Process for CCTV Management and Operators.

3.3 Responsibilities

- The School is the Data Controller and is legally responsible for compliance with the GDPR and DPA
- The Principal has overall responsibility for ensuring compliance with this policy
- Responsibility for deciding which information is recorded, how it will be used and to whom it may be disclosed has been delegated to the Bursar
- The Head of Estates and Property Services, Head Janitor and Assistant Head Janitor are identified as authorised personnel, also known as 'CCTV Managers' and 'CCTV Operators' in certain circumstances, such as the use and control of the equipment and viewing the live or recorded images. This ensures that the sharing of personal data is kept to a minimum within the School
- Day-to-day operational responsibility for CCTV cameras and the storage of data recorded is the responsibility of the Head of Estates and Property Services
- The Estates and Property Services Department, under the guidance of the Bursar, is responsible for identifying the most suitable place to locate the cameras. The cameras will not process data that may be deemed as 'excessive', such as capturing public areas outside the scope of the School, or where there is a reasonable expectation of privacy such as toilets or staff rooms, as this goes beyond what is proportionate and necessary to fulfil the purpose for processing the personal data
- The School's authorised personnel are responsible for ensuring that the cameras are working correctly and consistently and will be responsible for ensuring they are maintained.

3.4 Storing and Viewing Images

- CCTV footage is stored securely and access is protected and limited to authorised personnel
- CCTV footage will be kept for a maximum of 30 days, unless an incident has occurred on School premises and the footage is to be kept for a purpose
- CCTV viewing may be carried out on occasion outside School hours by on-duty Janitorial staff for specific instances (e.g. investigation of an alarm, or a report of a disturbance). On such occasions the CCTV Footage Disclosure Register will be completed retrospectively
- CCTV viewing by unauthorised or unqualified staff will be carried out in accordance with the relevant procedure ensuring that privacy and data protection is maintained
- CCTV can record personal data in the form of a person's face and may indicate 'special category' personal data, such as a person's ethnic origin or physical disability. This means that live or recorded images and monitor screens will not be viewed by any unauthorised third party without a lawful basis i.e. the person(s) that appear and are identifiable from the footage.

3.5 Disclosure of Images

The School will ensure that any disclosure of images is done in a controlled manner and that the disclosure is consistent in regards to CCTV. Any disclosure will be clearly documented by the School as outlined in Annex A - CCTV Process for CCTV Manager and Operators, Annex B - CCTV Procedure (Internal) and Annex C - CCTV Procedure (External) depending on the type of request and disclosure.

There will be no disclosure of recorded data to third parties without a lawful basis. It is acceptable for the School to disclose images to law enforcement agencies for the purpose of prevention and detection of crime. These requests are to be:

- Provided in writing to the Principal or Bursar, where possible
- Signed by authorised officers
- Make reference to the name and section of the legislation that entitles them to receive the information.

If the immediate viewing of a recording is necessary, this will be governed by the relevant procedures and in accordance with clause 3.5

In cases where disclosure is requested by a third party who does not appear on the footage, extreme caution must be taken and referred to the Bursar. Where this is a parent on behalf of a pupil, the Subject Access Guidance will be followed. Where technology permits, images of third parties will be blurred and unidentifiable if a disclosure request does not pertain to them.

The data may be used within the School's Disciplinary and/or Complaints Procedures as required, and will be subject to the normal confidentiality requirements of those procedures.

3.6 Authorised Personnel

All authorised operators and employees with access to images must be aware of the procedures that need to be followed when accessing the recorded images. Authorised personnel will be trained and certified in the use of CCTV.

The viewing of all images from our CCTV system must be controlled and consistent with the purpose for which the system was installed. On a routine basis, this means that teaching and unauthorised support staff cannot request access to footage.

On occasion the School may receive a request to carry out covert monitoring on behalf of the Police, which must be requested with evidence of the Police's RIPA authorisation for this surveillance and authorised by the Bursar. If this is not possible due to sensitivity issues, the authorised personnel will consider escalation.

Appropriate personnel will allow third parties to view live and recorded images for maintenance purposes and in compliance with the objectives of the CCTV objectives set out in paragraph 3.4.

The School's Bursar may be involved in any circumstances where the School feels advice is necessary. Where the School is unsure of whether to seek advice from the Bursar, for the avoidance of doubt advice is to be sought.

3.7 Breaches

A 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Any breach of CCTV security will be initially investigated by the School's appropriate personnel, in order to discuss this further with the School's Bursar, governing body and Principal's Leadership Team. The School's Bursar may initiate communications to the ICO within the 72 hour period in cases where the breach could lead to or has led to a risk of harm. The Bursar may extend the communications to those affected by the breach, in order to provide them with the details in regards to the breach of their personal information and how they can take precautions from further consequences of the breach.

A breach of this policy will be investigated under the School's existing policies and procedures. Any serious breach of the CCTV Policy may be considered as a form of gross misconduct. This investigation will involve the input of the School's Bursar.

A breach of security in relation to CCTV footage will be actioned in line with the Critical Security Incident Response Procedure.

Where a criminal offence has been committed on School premises, the School is not under any duty to release the footage to or allow it to be viewed by the subject, their family or friends. Any unauthorised disclosure of the footage may prejudice any subsequent police enquiry.

When an incident occurs on School premises during evenings or weekends and access to CCTV is required, it is necessary to contact the Head of Estates and Property Services or other authorised personnel.

CCTV will only be accessed via authorised personnel using multi-factor authentication which helps to minimise chances of a data breach. The CCTV Manager will routinely check access logs to ensure there is no unauthorised access

3.8 CCTV and GDPR

In order to comply with the right to be informed, signage is displayed in prominent positions in all access points to the School to inform staff, visitors, parents and pupils and the general public that they are entering an area where their images are being recorded either as still or video footage. Employee, parent, pupil and visitor privacy notices include the information that the School uses CCTV cameras. Visitors must have the knowledge of who to contact to make an enquiry regarding the system where this is not obvious.

The right for individuals to request access to their data can be exercised using a subject access request (see section 3.10 below).

The right to object/restrict processing may be possible in certain circumstances. However, this will be considered on a case by case basis.

The right to rectification will apply where possible (a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete).

The right to data portability (allows data subjects to obtain data that a data controller holds on them and to reuse it for their own purposes) is not applicable as CCTV is filmed under the public task duty. Automated decision making is not included in this process.

Data minimisation is exercised with the automated deletion of CCTV footage after 30 days or less, unless an exemption to the rule applies, for example, a police investigation is ongoing.

The right to erasure (i.e individuals have the right to have personal data erased) is considered where the personal data is no longer necessary in relation to the purposes for which it was processed.

All rights can be exercised by individuals through contacting the Bursar.

3.9 Retention and disposal

CCTV images will not be retained for longer than necessary, taking into account the purposes for which they are being processed. Data storage is automatically managed by the CCTV digital records which overwrite historical data in chronological order to produce a 30-day rotation in data retention.

If there is a legitimate reason for retaining the CCTV images (such as for use in an accident investigation, disciplinary investigation and/or legal proceedings), the footage or still frames can be isolated and saved in a secure encrypted file. Any saved images or footage will be stored securely and deleted once they are no longer needed for the purpose for which they were saved.

3.10 Subject Access Requests

Individuals have the right to request access to CCTV footage relating to themselves under the GDPR and DPA. The Subject Access and ICO guidance will be followed.

All requests are to be made in writing to the Bursar and must include sufficient information to enable the footage relating to them to be identified. For example, date, time and location.

Where a Subject Access Request includes footage of another individual not included in the request, the School will either use 'blurring' to distort the images to only the relevant individual; or gain consent to disclose third party personal data from those individuals not involved in the request.

The School reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an ongoing investigation.

Wherever possible, the Bursar will notify the requester if an exemption or limitation to their request applies, such as, but not limited to:

- A claim to legal professional privilege in legal proceedings
- The request will infringe on a third party's rights and freedoms
- Any other exemption to the right of access as stated in the GDPR and DPA.

3.11 Complaints

If a person is not satisfied with the way that we have handled their requests or questions relating to our use of personal data then they can either raise a complaint under the School's Complaint Procedure.

The Information Commissioner's Office is the statutory body responsible for overseeing data protection legislation and law in the United Kingdom.

3.12 Review and Implementation

The Head of Estates and Property Services is the owner of this Policy and it will be reviewed every two years with input from the Head of IT Services and Bursar where appropriate.

The Principal's Leadership Team will approve this policy.

The School will make this CCTV Policy available via the Parent and Staff Portals.

Owner	Title	Date	Signature
Karen McPhillips	Head of IT	??/??/2022	
Scott Muir	Head of Estates and	??/??/2022	

	Property Services		

Approved By	Title	Date	Signature
James Mills	Bursar	??/??/2022	

Version	Date last reviewed	Reviewer	Notes
V1.0 DRAFT	29/06/2020	Karen McPhillips	Initial draft complete
V2.0 DRAFT	??/??/2022	Karen McPhillips	Complete rewrite, adding procedures

Other Key Documents

Data Retention Policy
Information Security - Overarching Policy
Privacy Notices - Working for Us
Privacy Policy - Educating Your Child
Privacy Policy - Keeping in touch
Privacy Policy - Galleon membership
Privacy Policy - Contacting us
Privacy Policy - Swire
Privacy Policy - Malawi Partnership
Complaint Policy and Procedure
Disciplinary Policy

How to contact the School with a CCTV query

If any member of staff, a pupil, parent/carer, or member of the public who reasonably believes they may have been captured by our CCTV cameras, has questions about this policy or any concerns about the Schools use of CCTV they should contact:

The Bursar
George Watson's College
Colinton Road
Edinburgh
EH10 5EG
or
dataprotection@gwc.org.uk or 0131 446 6000

Annex A - CCTV Disclosure Procedure for CCTV Manager and Operators

DPIA

- The School will document in their DPIA how personal information will be shared and complete a relevant DPIA for any new camera or changes to an existing camera
- In deciding whether to carry out a DPIA and its scope, consideration must be given to the nature and scope of the surveillance camera activities and their potential to interfere with the privacy rights of individuals.
- You must carry out a DPIA for any processing of surveillance camera data that is likely to result in a high risk to individual privacy. The GDPR states that a DPIA "shall in particular be required in the case of:

  systematic monitoring of publicly accessible places on a large scale" (Article 35).

  Furthermore, as a controller in relation to the processing of personal data, you must seek the advice from the Data Protection Officer/Bursar when carrying out a DPIA and if cases such as:

  - Before any new system is installed
  - Whenever a new technology or functionality is being added on to an existing system
  - Whenever there are plans to process more sensitive data or capture images from a different location.

CCTV Requests

- If any of the Estates and Property Services team receive a verbal or email request for internal CCTV disclosure, the individual must ask the requestor to follow Annex B - CCTV Disclosure (Internal)
- If the Head of Estates and Property Services or appropriate person receives a request from the police, but it is not an emergency, the request will be directed to the School's email address to be dealt with during normal office hours under Annex C - CCTV Disclosure (External)
- On receipt of a 'routine' subject access request by an individual, the Head of Estates and Property Services or appropriate person must ask the requestor to submit a 'Subject Access Request to the Bursar as outlined in Annex C - CCTV Disclosure (External) linked above.

Disclosing Footage

- When conducting a viewing, either of live images or recorded playback, viewing of CCTV footage will take place in a secure office environment and only those persons who are authorised and/or who appear on the footage are to be present where relevant
- CCTV Operators must ensure that no part of the footage can be seen through a window in a door or a window looking into the office from an external area
- The office door will be completely closed for the duration of the viewing and for any discussions about the footage that may follow
- If an incident has occurred, the footage in question must be stored securely in a way that maintains the integrity of the images pending further action
- The School has developed a register called the "CCTV Footage Disclosure Register" and it must be completed on every occasion that footage is viewed or disclosed to a third party
- Once the action/investigation has been concluded, a review of the retention of the footage will be exercised by the CCTV Manager and/or CCTV Operator. The CCTV Manager will ensure secure and permanent disposal of the footage occurs where there is no longer a valid lawful basis to keep the images.

Security

- To check CCTV is being accessed appropriately, with authorisation and minimise the chances of a data breach, the CCTV Manager will scan the access logs monthly and investigate any unauthorised access. In the case of a potential breach, the CCTV Manager must follow the Information Security - Security Incident Management Policy and Procedure
- The CCTV Manager and CCTV Operators must use Multi-factor authentication when accessing CCTV system as part of the Information Security guidelines.

Annex B - CCTV Disclosure Procedure (Internal)

CCTV disclosures must follow a formal procedure to comply with GDPR legislation, Data Protection and formal record keeping for information security.

1. Requestor must raise a ticket in TopDesk to request access to CCTV
2. The requestor will complete the form with the following information
    a. Purpose of the request
    b. Date and time of incident
    c. Location of incident
    d. Justification for requesting access/information
3. The CCTV Manager or member of the Estates team will review the request and will send it to Bursar or COO for approval.
4. The Bursar or COO will provide decision and reason for decision (within the ticket for tracking purposes)
5. Once decision is made, the CCTV Manager or member of the Estates team will either;
    - Inform the requester that the request has not been approved with justification for the decision then close the case on TopDesk
      or
    - Delegate to CCTV Operator to retrieve footage and provide information to requestor (it may be necessary to blur out any other non relevant person(s) and update the ticket with details of the date, time and name of operator access and providing the footage then close the TopDesk ticket.
6. The CCTV Manager or CCTV Operator will log the disclosure of information in the "CCTV Footage Disclosure Register" is completed detailing;
    a. Entry number
    b. Date
    c. Name of Authorised Person
    d. Name of person requesting footage
    e. Purpose of request
    f. Authorised by and justification
7. The authorised person in the CCTV footage disclosure will then review the relevant camera footage, ensuring they are complying with Annex A - CCTV Disclosure Procedure for CCTV Manager and Operators.

Annex C - CCTV Disclosure Procedure (External)

Subject Access Requests will follow the School's Subject Access Request Procedure If the request is pertaining to CCTV disclosure this will follow the procedures outlined below.

When disclosing in regard to insurance purposes or law enforcement requests, this procedure must be followed;

1. The following information will be required after receiving an external request and may require follow-up to gather details:
    a. purpose of the request
    b. Date and time of incident
    c. Location of incident
    d. Justification for requesting access/information
2. The CCTV Manager will send it to Bursar or COO for review and approval.
3. The Bursar or COO will provide a decision (Approved or Rejected) and a reason for this decision.
4. Once decision is made, the CCTV Manager will:
    - Inform the requester that the request has not been approved with justification for the decision or
    - Delegate to CCTV Operator or carry out the investigation to view and retrieve footage .
5. The CCTV Manager or CCTV Operator will log the disclosure of information in the "CCTV Footage Disclosure Register" is completed detailing;
    a. Entry number
    b. Date
    c. Name of Authorised Person
    d. Name of person requesting footage
    e. Purpose of request
    f. Authorised by and justification
    g. Date of release of footage
    h. Date of investigation closed and footage destroyed
6. The CCTV Manager or CCTV Operator will then download the recording pertaining to the request onto a portable device and securely stored in a locked room until collection.
7. The file must be encrypted or password protected. Alternatively, if requested, the recording will be sent in a password protected document via email.
8. CCTV Manager or Operator will ensure the password(s) are given to the authorised recipient separately from the email containing the recording, ensuring that the original copy of the recording is kept at the School for only as long as is necessary for the purpose of retaining the recording.
9. Where an external request includes footage of another individual not included in the request, the School will either use 'blurring' to distort the images to only the relevant individual; or gain consent to disclose third party personal data from those individuals not involved in the request. This may require additional support from the specialist AV unit to use appropriate software and tools to blur/distort images of individuals not included in the investigation. Normally, an associated crime reference number will be provided with the request.

Process Flow (Internal Flow)

Requesting (via Email or in person)

a. What is the purpose of the request
b. Location of the incident
c. Date and Time of the incident
d. Please provide full details of the incident and alleged subjects you require footage of?
    i. Length of recording
    ii. Details of all subjects
    iii. Detailed description of each subject
    iv. Detailed description of the alleged incident
e. Justification for requesting disclosure of this footage

Authorisation Request

f. Enter comments into last action entry box for Bursar / COO
g. Change the processing status to "waiting for user" (waiting for Bursar/COO)
h. When the email window pops up, change the email address to dataprotection@gwc.org.uk or s.breadner@gwc.org.uk
i. Requesters will be able to follow the process as they automatically receive emails of progress.

Approval/Rejection

j. Bursar or COO will respond back via email with approve or reject, If rejected, Bursar or COO must provide reason for rejection
k. If rejected, update the last action box referring to the decision then mark the processing status to complete then click on save to close the ticket
l. If approved, the Estates team can proceed then update and close the ticket accordingly and move to releasing/viewing

Releasing/Viewing

m. Date(s) and time(s) at which access was allowed/or disclosure made;
n. The CCTV Manager or delegated CCTV Operators providing access; Name, Date and Time
o. The "CCTV Footage Disclosure Register" is completed detailing;
    i. Entry number
    ii. Date
    iii. Name of Authorised Person
    iv. Name of person requesting footage
    v. Purpose of request
    vi. Details of recorded footage (Date, times)
    vii. Footage viewed on site or removed
    viii. Type of recording taken (CCTV Image, Video or Video with Audio)
    ix. Date copied footage removed from site or reviewed internally
    x. Authorised Y/N
    xi. Justification
    xii. Case Closed Y/N

Closure

p. The register is 're-shared' with the Data Protection Officer/Bursar ensuring an automated notification Email is sent.
q. Information passed to the requestor in a secure and/or encrypted format.
r. Date/Time case closed
s. Confirmation of Image/Recording deletion

Process Flow

Requesting (via Email or in person)

t. What is the purpose of the request
u. Location of the incident
v. Date and Time of the incident
w. Please provide full details of the incident and alleged subjects you require footage of?
    i. Length of recording
    ii. Details of all subjects
    iii. Detailed description of each subject
    iv. Detailed description of the alleged incident
x. Justification for requesting disclosure of this footage

Authorisation Request

y. Enter comments into last action entry box for Bursar / COO
z. Change the processing status to "waiting for user" (waiting for Bursar/COO)
aa. When the email window pops up, change the email address to dataprotection@gwc.org.uk or sbreadner@gwc.org.uk
bb. Requesters will be able to follow the process as they automatically receive emails of progress.

Approval/Rejection

cc. Bursar or COO will respond back via email with approve or reject, If rejected, Bursar or COO must provide reason for rejection
dd. If rejected, update the last action box referring to the decision then mark the processing status to complete then click on save to close the ticket
ee. If approved, the Estates team can proceed then update and close the ticket accordingly and move to releasing/viewing

Releasing/Viewing

ff. Date(s) and time(s) at which access was allowed/or disclosure made;
gg. The CCTV Manager or delegated CCTV Operators providing access; Name, Date and Time
hh. The "CCTV Footage Disclosure Register" is completed detailing;
    i. Entry number
    ii. Date
    iii. Name of Authorised Person
    iv. Name of person requesting footage
    v. Purpose of request
    vi. Details of recorded footage (Date, times)
    vii. Footage viewed on site or removed
    viii. Type of recording taken (CCTV Image, Video or Video with Audio)
    ix. Date copied footage removed from site or reviewed internally
    x. Authorised Y/N
    xi. Justification
    xii. Case Closed Y/N

Closure

ii. The register is 're-shared' with the Data Protection Officer/Bursar ensuring an automated notification Email is sent.
jj. Information passed to the requestor in a secure and/or encrypted format.