Global Banking School
+44 (0) 207 539 3548
info@globalbanking.ac.uk
www.globalbanking.ac.uk
891 Greenford Road, London
UB6 0HE

GBS CCTV Policy and Procedures

Version Control

Document title	GBS CCTV Policy and Procedures
Oversight Committee	Executive Board
Policy lead (Staff member accountable)	Managing Director
Approved by	Executive Board
Approval date	February 2022
Date effective from	February 2022
Date of next review	February 2025
Version	1.0

Related GBS policies
▪ GBS Student Charter ▪ GBS Student Code of Conduct ▪ GBS Student Disciplinary Policy ▪ GBS Staff Disciplinary Policy ▪ GBS Records Management and Retention Policy ▪ GBS Anti-Harassment and Anti-Bullying Policy ▪ GBS Data Protection Policy ▪ GBS Privacy Policy ▪ GBS Data Subject Access Request Policy ▪ GBS Access Control Policy ▪ GBS ICT Policy ▪ GBS Safeguarding Policy
External Reference Points
1. Information Commissioner's Office, Accessed online at: https://ico.org.uk/ 2. UK Public General Acts, *Data Protection Act 2018*, Accessed online at: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted 3. UK Public General Acts, *Equality Act 2010*, Accessed online at: https://www.legislation.gov.uk/ukpga/2010/15/contents 4. UK Public General Acts, *Freedom of Information Act 2000*, Accessed online at: https://www.legislation.gov.uk/ukpga/2000/36/contents 5. UK Public General Acts, *Protection of Freedoms Act 2012*, Accessed online at: https://www.legislation.gov.uk/ukpga/2012/9/section/29/enacted#:~:text=%20Protection%20of%20Freedoms%20Act%202012%20%201,different...%205%20%287%29%20In%20this%20section%E2%80%94%20More%20 6. UK Public General Acts, *Human Rights Act 1998*, Accessed online at: https://www.legislation.gov.uk/ukpga/1998/42/contents 7. The Surveillance Camera Commissioner's Office (SCCO), *Code of Practice*, Accessed online at:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/282774/SurveillanceCameraCodePractice.pdf
8. Information Commissioner's Office, *The employment practices code,* Accessed online at: https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

Contents

Global Banking School CCTV Policy and Procedures

1. Introduction and Scope

1.1 Global Banking School (GBS) as a data controller is the owner and operator of the Closed-Circuit Television (CCTV) monitoring on all its campuses. This policy details the operating procedures and standards for the use of CCTV and offers a legitimate role in maintaining a safe and secure environment for all our students, staff, and visitors. GBS recognises that this may raise concerns about the effect on individuals and their privacy. This policy is intended to address those concerns through appropriate management and operation of CCTV systems at GBS, with reference to GBS Safeguarding (Prevent) Policy.

1.2 This policy will incorporate the main regulations which govern the use of CCTV. Due to the potentially sensitive nature of surveillance, there are codes, guidelines and legislation which must be complied with to operate a CCTV scheme legally and fairly. Images captured on CCTV are personal data, which must be processed in accordance with GBS Data Protection Policy. GBS is committed to complying with its legal obligations and ensuring that the legal rights of all GBS members (students, staff, and visitors) are recognised and respected.

2. Purpose

2.1 The use of CCTV at all GBS's campuses is intended to provide an increased level of security environment for the benefit of those who visit, study and work on all our campuses. The CCTV system is intended to view, monitor, and record activities within GBS premises. It will focus primarily, but not limited to, key entry and exit points to premises, building perimeters, certain communal areas, and other parts where CCTV is recommended to mitigate against risks to safety and security. Every possible effort has been made in the planning and design of the CCTV system to give it maximum effectiveness. However, it is not possible to guarantee that the system will see every single incident taking place in the areas of coverage.

2.2 The CCTV system must strike an appropriate balance between the personal privacy of individuals using the campuses/buildings and the objective of recording incidents. The system will be operated fairly to ensure that all CCTV data is processed in accordance with UK GDPR, the Data Protection Act 2018, and GBS Data Protection Policy and only for the purposes to which it is established.

2.3 The system is not intended to invade the privacy of any individual in residential, business, or other private premises, buildings or land not belonging to GBS. CCTV is not used to record conversations. No images will be captured in areas where individuals would have an expectation of privacy (for example, toilets, showers, changing facilities etc.).

2.4 GBS uses CCTV systems essentially:

a) To act as a deterrent against crime and safeguarding public, student, and staff safety.
b) To protect buildings and assets from damage, disruption, or vandalism.
c) Assist in investigating and detecting crime or reports of possible crime.
d) To gather evidence by a fair and accountable method.
e) Facilitate the identification, apprehension and prosecution of offenders or suspected offenders.
f) Protect GBS Security staff from threats and violence.
g) Assist in safeguarding GBS staff (and any other persons in the premises) during emergency situations.
h) Support the investigation of safety and security-related incidents and suspected misconduct by staff, students, or visitors.
i) Provide law enforcement bodies or GBS with evidence which may lead to possible criminal, civil or disciplinary action against either staff, students, or visitors.
j) Provide evidential material for use in potential criminal, civil or disciplinary actions including employment tribunal proceedings.
k) Facilitate the investigation of any suspected breaches by GBS or staff of their respective obligations and rights in connection with employment.
l) To assist with Health and Safety.
m) Assist in the effective resolution of disputes which arise during grievance proceedings; and
n) To monitor traffic management, including monitoring parked vehicles, facilitating car parking and enforcement of GBS regulations.

2.5 This list is not exhaustive and other purposes may become relevant.

3. Legal Framework

3.1 This policy sets out how GBS will handle the personal data of our staff, clients, suppliers, partners, employees and other third parties. The legal framework that governs this policy is founded on the following acts: The Data Protection Act (DPA) 2018, The United Kingdom General Data Protection Regulation (UK GDPR) which regulates how personal data can be processed and protected. Data Protection law ensures that CCTV cameras are used only where and when it is necessary, which is arguably one of the most fundamental elements of legal compliance. The DPA explicitly states that personal data "shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed."[1]

3.2 The Information Commissioner's Office (ICO) is a government body and provides a compilation of practical advice about how to ensure GBS is following data protection guidelines. The ICO issues data protection code of practices for surveillance cameras and personal information which has been crucial in compiling this policy.

3.3 Section 40 of the Freedom of Information Act (FOI) 2000 contains a two-part exemption relating to information about individuals and regulates access to information held by public authorities. The Protection of Freedoms Act (POFA) 2012 regulates (among others) how surveillance and biometric data can be used, and how these types of data must be safeguarded. The Human Rights Act (HRA) 1998 includes provisions regarding the right to privacy.

3.4 The Surveillance Camera Commissioner's Office (SCCO) also issued a Code of Practice, aiming not only to detail the legal requirements that CCTV users are bound by, but also to provide a coherent technical framework for planning the deployment of CCTV cameras and for integrating them in our security system. (*Please refer to APPENDIX C - The Surveillance Camera Commissioner Code of Practice: A guide to the 12 principles for more information*).

4. Roles and Responsibilities

4.1 GBS is registered with the Information Commissioner's Officer as a Data Controller. Details of the School's registration are published on the Information Commissioners

[1] Data Protection Act 2018 Sch I, 3.

website. GBS as a Data Controller shall implement appropriate technical and organisational measures to ensure that processing of personal information alongside CCTV is performed in accordance with the UK GDPR and DPA (2018). GBS as a data controller of a CCTV system has the following responsibilities:

- To ensure that surveillance camera systems are used only where and when it is necessary.
- To ensure an effective administration of the surveillance system.
- To ensure that the data is guarded against unauthorised access.
- To ensure that the data is disclosed to those who have the legal right to access.
- To retain the data only as long as it is legitimately needed.
- To inform surveillance subjects about the use of surveillance equipment, about their rights and about the procedures that they need to follow to obtain any data that they are legally entitled to.

4.2 Roles and responsibilities include:

- GBS Senior Management Team: Responsible for ensuring that their staff are made aware of this policy and that breaches are dealt with appropriately and developing and encouraging good information handling practices within their areas of responsibility.

- Information Commissioner's Office ("ICO"): ICO is the Independent Regulatory Office in charge of upholding information rights in the interest of the public. The organisation covers the Data Protection Act and advises businesses on how to comply with UK GDPR and therefore requires every data controller who is processing personal information to register with the ICO.

- GBS Duty Control Room Operator (Security)-Responsible for operating and maintaining surveillance equipment, watching both live and recorded video surveillance footage, reporting incidents or suspicious behavior to GBS Data Protection Officer/GBS Senior Management Team and/or public authorities where necessary. They must also maintain the control room equipment, watching multiple monitors at once, making note of any unusual occurrences. GBS staff using CCTV systems are given appropriate Data Protection training to ensure

they understand and observe the legal requirements related to the processing of relevant data. Any misuse, or wrongful processing, of the relevant data could result in disciplinary action.

- GBS Data Protection Officer**:** DPO is responsible for advising GBS on its obligations, monitoring compliance, assisting with Data Protection Impact Assessments (DPIAs) and liaising with the Information Commissioner's Office. The DPO is also responsible for ensuring that GBS processes the personal information of its staff, students, customers, providers, and partners in compliance with the applicable data protection rules. Any issues related to Data Protection and compliance issues, please contact dpa@globalbanking.ac.uk.

- GBS Head of Facilities, GBS Human Resources: Responsible for implementation, monitoring and review of this policy and ensuring that training, guidance, and advice regarding data protection compliance is made available to staff.

- GBS Line Managers**:** Responsible for ensuring that requests made under data subject rights are reviewed and where appropriate referred to Human Resources promptly and ensuring that suspected or actual compromises of personal data are reported immediately.

- All GBS Members (staff and students)- All members of staff and students are advised to familiarise themselves with this policy and the appropriate GBS Privacy Policy and GBS Data Protection Policy. Any issues related to Data Protection and compliance issues, please contact dpa@globalbanking.ac.uk.

5. Control Room Access

5.1 CCTV cameras will be monitored by a CCTV control-room which is based at GBS Greenford campus, 891 Greenford Road, Greenford, West London, UB6 0HE.

5.2 GBS CCTV cameras are in various areas around the campus positioned both internally and externally in all locations where GBS operates including GBS London (Republic, Stratford, Bow and Greenford campus), GBS Birmingham, GBS Leeds and GBS Manchester campuses. These will monitor our academic buildings (including individual and open plan offices), libraries, classrooms, computer

laboratories, student and staff social/communal areas, security rooms, reception areas, and car parks etc.

5.3 Access to recorded images will be restricted to those staff authorised to view them and will not be made more widely available. CCTV access will be restricted to:

- GBS Duty Control Room Operator (Security)
- GBS Chief Executive Officer
- GBS Managing Director
- GBS Head of IT
- GBS Data Protection Officer
- Statutory bodies such as Police, Health and Safety Executive (HSE), etc.
- Any other person with interest must obtain authority from GBS Data Protection Officer to view recorded footage, providing reasons and justification.

5.4 All security staff involved in the recording, observation and capture of images must act in an ethical and lawful manner in accordance with legislation and must receive adequate training to ensure their understanding of compliance legislation. Training will include how to identify suspicious behaviour, when to track individuals or groups and when to take close views of incidents or people and compliance with Data Protection Act and any other relevant legislation.

5.5 Staff with access to CCTV data should be particularly careful not to infringe upon the Human Rights Act 1998. The access permission rights will be reviewed regularly and will change depending on the circumstances.

6. Monitoring and Recording

6.1 CCTV is checked daily by GBS Duty Control Room Operator (Security) to ensure that images remain fit for purpose and that the data and time stamp recorded on images is accurate. GBS intended use is to capture images of intruders or of individuals damaging property or removing goods without authorisation or of anti-social behaviour. The CCTV system will be operated 24 hours a day, 7 days a week, every day of the year.

6.2 Where new CCTV systems or cameras are to be installed, GBS will carry out a full Data Protection Impact Assessment (DPIA) identifying risks related to the installation and ensuring full compliance with data protection legislation. CCTV will be installed in communal areas, reception areas, student areas and areas where students interact with staff.

6.3 GBS will ensure that all cameras are set up in a way that ensures minimal intrusion of privacy, and that any intrusion is fully justified. No images and information will be stored beyond those which are strictly required for the stated purpose of a CCTV system.

6.4 CCTV images and information will be subject to appropriate security measures to safeguard against unauthorised access and use.

7. Signage

7.1 It is a requirement of the Data Protection Act 2018 to notify people entering a CCTV protected area that the area is monitored by CCTV and that pictures are recorded. Strategically placed CCTV camera notices at key entry points will advise individuals that they are entering an area which is covered by CCTV cameras. GBS must ensure that this requirement is fulfilled. The CCTV sign should include the following:

- Include the operator details and a contact telephone number for any enquiries: Global Banking School (data controller)
- Be clearly visible, legible and be of a size appropriate to the circumstances.
- Confirm that the area is covered by CCTV surveillance and pictures are recorded.
- State the purpose of using CCTV.

7.2 Signage shall be placed internally in each GBS campuses/premises near to where CCTV cameras are sited to inform all GBS members (data subjects) that CCTV is in operation in that area. Appropriate locations for signage will include:

- Entrances to premises e.g., external doors, walls, and any highly visible appropriate area.
- Reception area.

- Close to each internal camera.

7.3 Please refer to APPENDIX D for CCTV Signage.

8. Covert Monitoring

8.1 GBS will inform data subjects on the sound legal basis that CCTV monitoring is being conducted through policies, privacy notices and signage unless, in exceptional circumstances for the prevention or detection of criminal activity or equivalent malpractice and any of the below from the ICO's guidance.

8.2 The ICO's Employment Practices Code defines covert monitoring as 'calculated to ensure that those subject to it are unaware that CCTV monitoring is taking place'. Covert monitoring should not normally be considered, and it will be rare for covert monitoring of workers to be justified. It should therefore only be used in exceptional circumstances such as:

- Strictly targeted at obtaining evidence within a set timeframe and that the covert monitoring does not continue after the investigation is complete.
- If embarking on covert monitoring with audio or video equipment, ensure that this is not used in places such as toilets or private offices.
- There may be exceptions to this in cases of suspicion of serious crime but there should be an intention to involve the police.
- In a covert monitoring exercise, limit the number of people involved in the investigation.
- Prior to the investigation, set up clear rules limiting the disclosure and access to information obtained.
- If information is revealed during covert monitoring that is tangential to the original investigation, delete it from the records unless it concerns other criminal activity or equivalent malpractice.

9. CCTV Storage and Retention

9.1 The Data Protection Act 2018 does not prescribe any specific minimum or maximum retention periods which apply to all systems or footage. Rather, retention should reflect GBS purposes for recording information. The retention period should be informed by the purpose for which the information is collected and how long it is needed to achieve this purpose. The Data Protection Act states that data '*shall not be kept for longer than is necessary for*' the purposes for which it was obtained.

9.2 As a data controller, GBS needs to be able to justify this retention period. For a normal CCTV security system, it would be difficult to justify retention beyond a calendar month (30 days), except where the images identify an issue, such as a break-in or theft and those images/recordings are retained specifically in the context of an investigation/ prosecution of that issue.

9.3 Accordingly, the images captured by GBS CCTV system will be retained for a maximum of 30 days. It will be overwritten automatically as the disk space is used up. If an incident is recorded that could give rise to claims against GBS, these recordings must be kept for a period of 6 years from the date of recording.

9.4 Retention periods must be established for required and non-required images, and secure and controlled storage and access arrangements for images. These must be discussed with the Data Protection Officer, and must consider the following points:

- Data storage is automatically managed by the CCTV digital recorders, which uses software programme to overwrite historical data in chronological order to enable the recycling of storage capabilities. This process produces an approximate 30-day rotation in data retention.
- Provided that there is no legitimate reason for retaining the CCTV images (such as for use in legal proceedings), the images will be erased following the expiration of the retention period.
- If CCTV images are retained beyond the retention period, they are to be stored in a secure place to which access is controlled.
- While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded.
- Systematic checks must be carried out to ensure compliance with the agreed retention period.
- Footage produced as part of a criminal, civil or disciplinary case will be retained for a minimum of 6 months after closure of the case.
- Hard drives and other media must be destroyed securely as confidential waste, except where the image identifies an issue.
- The images/recordings will be stored on a password-protected, secure network video device.

9.5 When images are removed for use in legal proceedings the following information must be logged:

- Date on which images were removed.
- The reason why they were removed.
- Any relevant crime incident number.
- The location of the images.
- Signature of the collecting police officer (if appropriate).
- Access to recorded images must be restricted to the designated member of staff responsible, who will decide whether to allow disclosure to third parties in accordance with GBS Access Control Policy.
- Viewing of recorded images must take place in a restricted area with controlled access.

9.6 For more information on our Data Retention Schedule, please review GBS Records Management and Retention Policy.

10. Data Subject Access Requests

10.1 Data Subjects may make a request for disclosure of personal data which may include CCTV images (a “Data Subject Access Request”). A Data Subject Access Request is subject to the statutory conditions, in accordance with the GBS Data Subject Access Request Policy. *(Please refer to APPENDIX E - Example of a Subject Access Request).*

10.2 Any persons whose images are recorded have a right to view those images, and to be provided with a copy of those images, within one month of making a written Subject Access Request.

10.3 In order for GBS to locate relevant footage/recordings, any requests for copies of recorded images or audio must include the date and time of the recording, the location where the footage was captured and, if necessary, information identifying the Data Subject. Availability of images will be subject to the retention period.

10.4 Requests for access to (review), or disclosure of (i.e. provision of a copy), of images recorded on the CCTV systems from third parties (i.e. unauthorised persons) will

only be granted if the requestor falls within the following types of person/organisation:

- Data Subjects (i.e., persons whose images have been recorded by the CCTV systems)
- Law enforcement agencies (where the images recorded would assist in a specific criminal enquiry)
- Prosecution agencies (including GBS Line Managers during staff or student disciplinary proceedings)
- Relevant legal representatives of data subjects

10.5 Images from CCTV must not be forwarded to the media for entertainment purposes or be placed on the internet. Images will only be released to the media on the authority of GBS Senior Management Team and following advice from law enforcement agencies to support police investigations.

10.6 GBS reserves the right to obscure images and/or edit audio of third parties when disclosing recordings captured on CCTV Systems when responding to a Data Subject Access Request once the technology is available.

10.7 Any request for recorded images or audio other than by way of a Data Subject Access Request will be considered under the Freedom of Information Act 2000 (an "FOIA Request"). An FOIA Request is subject to the statutory conditions and should be made in writing. On receipt of a Data Subject Access Request or FOIA Request, the GBS Data Protection Officer shall advise GBS Senior Management Team whether any disclosure should be made.

11. Guidance and Related Policies

11.1 This policy is accompanied by the staff handbook and must be followed to achieve GBS policy objectives. Reference should also be made to the GBS Data Protection Policy, GBS Privacy Policy, GBS Records Management and Retention Policy, GBS Data Subject Access Request Policy, GBS Access Control Policy, GBS ICT Policy, and GBS Equality and Diversity Policy. Information on other related policies is available from GBS Academic Standards and Quality Office (ASQO).

12. Staff Training and Audit

12.1 This policy may be amended by GBS at *any time*. GBS will ensure that those staff responsible for monitoring CCTV footage receive appropriate training to enable them to comply with this policy and Data Protection Law. Data Protection training is mandatory. Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

12.2 Any individual who does not think they are sufficiently aware of Data Protection Law should contact GBS Human Resources to arrange additional training. GBS will regularly test our systems and processes to monitor compliance. For Data Protection purposes and compliance matters, please contact dpa@globalbanking.ac.uk.

13. Privacy Impact Assessment (PIA)

13.1 The use of CCTV footage will be critically analysed using a Privacy Impact Assessment (PIA) under the UK GDPR this will become a Data Protection Impact Assessments (DPIA), however will follow the same principles of a PIA.

13.2 The Data Protection Officer will evaluate the CCTV system annually and will consider the following:

- The assessment of impact upon crime and consider all operational, technical and competency standards, relevant to the CCTV system and its purpose, and work to meet and maintain those standards in accordance with the law.
- Assessment of areas without CCTV
- The views of the users
- Operation of the policy
- Whether the purposes for which the scheme was established still exist
- Future functioning, management, and operation of the CCTV system
- Be designed to take into account its effect on individuals and their privacy and personal data.
- Be subject to stringent security measures to safeguard against unauthorised access.

13.3 If the DPIA reveals any potential security risks or other data protection issues, GBS will have provisions in place to overcome these issues.

14. Breach

14.1 Breaches of the policy and of security will be investigated by GBS Senior Management Team or GBS Data Protection Officer. Recommendations and corrective action plans will be put in place to remedy any breach which is proven. All breaches of personal data must be reported to GBS Data Protection Officer who is responsible for maintaining a record of CCTV data breaches as part of the policy.

15. Complaints

15.1 Complaints and enquiries about the operation of CCTV within GBS premises should be directed to our GBS Data Protection Officer, please contact dpa@globalbanking.ac.uk.

15.2 Complaints by students should go through the standard complaint procedure which is readily available on our website GBS Complaints Policy and Procedure.

15.3 Complaints by staff, please refer to *APPENDIX F- GBS Staff Complaint Procedure Flow Chart*.

15.4 If the issue remains unresolved, and the complainant considers that GBS is not operating within the Code of Practice as issued by the Information Commissioners Office, they are advised to contact The Information Commissioners Office.

16. Alternative Format

16.1 This policy can be provided in alternative formats (including large print, audio and electronic) upon request. For further information, or to make a request, please contact:

- **Name:** Welfare Management Team
- **Position:** Welfare Officer/Manager
- **Email:** welfare@globalbanking.ac.uk

APPENDIX A

Glossary

CCTV (Closed Circuit Television): means fixed position, domed, pan, tilt and zoom (PTZ) cameras at both internal and external locations designed to capture and record images of individuals and property.

Data: is information, which is stored electronically, or in certain paper-based filing systems. In respect of CCTV, this generally means video images. It may also include audio recordings or static pictures such as printed screen shots.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data as a result of the operation of its CCTV (or other Surveillance Systems).

Data Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Data Controller of all Personal Data relating to GBS Personnel and Personal Data used in our business for our own commercial purposes.

Personal Data: Personal Data: 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. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location, or date of birth) or an opinion about that person's actions or behaviour. This will include video images/recordings of identifiable individuals.

PIA: privacy impact assessment processing is any activity which involves the use of Personal Data. It includes obtaining, recording, or holding Personal Data, or carrying out any operation on Personal Data including organising, amending, retrieving, using, disclosing or destroying it. Processing also includes transferring Personal Data to third parties.

Surveillance Systems: means any devices or systems designed to monitor or record images and, in certain cases, audio of individuals or information relating to individuals. The term includes

CCTV as well as automatic number plate recognition (ANPR), body worn cameras, and any other systems that capture information of identifiable individuals or information relating to identifiable individuals.

United Kingdom General Data Protection Regulation (UK GDPR): The United Kingdom General Data Protection Regulation ((EU) 2016/679). Personal Data is subject to the legal safeguards specified in the GDPR.

Data Protection Impact Assessments (DPIA): A Data Protection Impact Assessment (DPIA) is a process to help companies identify and minimise the data protection risks of a project. This is carried out for processing that is likely to result in a *high risk* to individuals regarding their personal data.

Information Commissioner's Office ("ICO"): ICO is the independent regulatory office in charge of upholding information rights in the interest of the public. The organisation covers the Data Protection Act and advises businesses on how to comply with UK GDPR and therefore requires every data controller who is processing personal information to register with the ICO.

Breach: any act or omission that compromises the security, confidentiality, integrity, or availability of Personal Data or the physical, technical, administrative, or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure, or acquisition, of Personal Data is a Personal Data Breach**.**

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with UKGDPR.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording, or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

Staff: all employees, workers, contractors, agency workers, consultants, directors, members, agency staff, temporary staff, work experience and volunteers and others.

Student: a person who is studying at GBS or other place of higher education to attain a particular qualification to help enter a particular profession.

Transparency Notices (also referred to as Fair Processing Notices) or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when GBS collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee Transparency Notices or the website privacy policy) or they may be stand-alone, one time privacy statements covering Processing related to a specific purpose.

APPENDIX B

Principles relating to the processing of Personal Data under Data Protection Act 2018 and UK GDPR

Personal data shall be:

a) Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.
b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
c) Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay.
e) Kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the personal data are processed; and
f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

APPENDIX C

The Surveillance Camera Commissioner Code of Practice: A guide to the 12 principles

How well does your organisation comply with the 12 guiding principles of the surveillance camera code of practice? Here are some questions you should consider to help you check if you comply. Please note, the below has been taken from [Code of practice - A guide to the 12 principles (publishing.service.gov.uk)](publishing.service.gov.uk) website.

1
- What's your system for?
- Do you review its use?

2
- Have you carried out a privacy impact assessment?
- Do you publish your privacy impact assessment?

3
- Do you have signage in place to say surveillance is taking place?
- Is there a published point of contact for people to raise queries or complaints with?

4
- Who's responsible for your system?
- Are your staff aware of their responsibilities?

5
- Do you have clear policies and procedures in place?
- Do your staff know what your policies and procedures are?

6
- How long do you keep images/information?
- How do you make sure images/information is deleted once they're no longer needed?

7
- Do you have a policy on who has access to the stored information?
- Do you have a policy on disclosure of information?

8
- Do you follow any recognised operational or technical standards?

9
- Do you make sure that the images captured by your system are caught securely?
- Are only authorised people given access to the images?

10
- Do you evaluate your system regularly to make sure it's still required?
- Could there be an alternative solution to a surveillance camera system?

11
- Can the criminal justice system use the images and information produced by your surveillance camera system?
- Do you have a policy on data storage, security and deletion?

12
- Do you use any specialist technology such as ANPR, facial recognition, Body Worn Video (BWV) or remotely operated vehicles (Drones)?
- Do you have a policy in place to ensure that the information contained on your database is accurate and up to date?

APPENDIX D

CCTV Signage

It is a requirement of the Data Protection Act 2018 to notify people entering a CCTV protected area that it is being monitored and that pictures are recorded. GBS must ensure that this requirement is fulfilled. The CCTV sign should include the following:

- Include the operator details and a contact telephone number for any enquiries: Global Banking School (data controller)
- Be clearly visible, legible and be of a size appropriate to the circumstances.
- Confirm that the area is covered by CCTV surveillance and pictures are recorded.
- State the purpose of using CCTV.

APPENDIX E

Example of a Subject Access Request

[Name and address of the organisation]

[Your name and full postal address]

[Your contact number]

[Your email address]

[The date]

Dear Sir or Madam

Subject access request

[Include your full name and other relevant details to help identify you].

Please supply the personal data you hold about me, which I am entitled to receive under data protection law, held in:

[Give specific details of where to search for the personal data you want, for example:

- my personnel file;
- emails between 'person A' and 'person B' (from 1 June 2017 to 1 Sept 2017)
- my medical records (between 2014 and 2017) held by 'Dr C' at 'hospital D';
- the CCTV camera situated at ('location E') on 23 May 2017 between 11am and 5pm; and
- financial statements (between 2013 and 2017) held in account number xxxxx.]

If you need any more information, please let me know as soon as possible.

[If relevant, state whether you would prefer to receive the data in a particular electronic format, or printed out].

It may be helpful for you to know that data protection law requires you to respond to a request for personal data within one calendar month.

If you do not normally deal with these requests, please pass this letter to your data protection officer or relevant staff member.

If you need advice on dealing with this request, the Information Commissioner's Office can assist you. Its website is ico.org.uk, or it can be contacted on 0303 123 1113.

Yours faithfully

[Signature]

Please note, the above subject access request example was obtained from the ICO website.

APPENDIX F

GBS Staff Complaint Procedure Flow Chart