The GORSE Academies Trust CCTV/Call-Recording Policy

Designated Person:	Director of Digital Strategy/Strategic Lead Officer
Reviewed by:	Policy Committee
Date:	March 2026
Version:	1.5

The GORSE Academies Trust, c/o John Smeaton Academy, Smeaton Approach, Barwick Road, Leeds, LS15 8TA
Chief Executive Officer: Sir John Townsley BA (Hons) NPQH
Deputy Chief Executive Officer: Mrs L Griffiths BSC (Hons) NPQEL
Chair of the Board: Mrs A McAvan BA (Hons) NPQH

0113 487 8888
info@tgat.org.uk
www.tgat.org.uk

CCTV Policy

The following amendments have been made to this version of the policy:

Section	Changes
Section 2	Additional section outlining the lawful basis for using CCTV.
Section 4	Information regarding the forms that covert monitoring in exceptional circumstances may take for transparency purposes.
Section 8	Further clarity regarding how the viewing of CCTV will take place.
Section 10	Inclusion of requests for CCTV footage from third parties such as the police.
Section 11	Additional section Commissioning and decommissioning procedure.
Section 12	Security of CCTV Images.
Section 13	Rights of Data Subjects
Section 14	Roles and Responsibilities

There are 3 elements to this policy and these are split into three distinct sections:

1. CCTV
2. In-Vehicle CCTV
3. Call-Recording

The GORSE Academies Trust
c/o John Smeaton Academy, Smeaton Approach, Barwick Road, Leeds, LS15 8TA
T 0113 487 8888 | **E**: info@tgat.org.uk | **W** www.tgat.org.uk

The GORSE Academies Trust

CCTV Policy

Designated Person:	Director of Digital Strategy/Strategic Lead Officer
Reviewed by:	Policy Committee
Date:	March 2026
Version:	1.5

The GORSE Academies Trust
c/o John Smeaton Academy, Smeaton Approach, Barwick Road, Leeds, LS15 8TA
T 0113 487 8888 | **E**: info@tgat.org.uk | **W** www.tgat.org.uk

CCTV POLICY

1. Introduction

1.1. This policy is written in accordance with the General Data Protection Regulation ("GDPR") which came into force on 25 May 2018 and the Data Protection Act 2018.

1.2. The GORSE Academies Trust ("GORSE") uses Closed Circuit Television ("CCTV") across its academies for the following purposes:

1.2.1. To assist in providing a safe and secure environment for all students, staff and visitors.

1.2.2. To assist in the prevention and detection of crime and to assist law enforcement with investigations and criminal proceedings.

1.2.3. To assist in the prevention and detection of theft and criminal damage to all assets within GORSE.

1.2.4. All cameras will be used to support positive behaviour in all academies and providing visual evidence of any incident as well as crime prevention and detection.

1.3. This policy is intended to provide protection against the misuse of CCTV systems within GORSE.

1.4. The CCTV system will never be used as part of any staff performance appraisal.

2. Lawful Basis

2.1. As with all instances where personal data is processed there must be lawful basis for doing so in line with the GDPR.

2.2. GORSE will process personal data through the medium of CCTV installations where necessary to pursue its legitimate interests and to carry out tasks in the public interest.

2.3. In particular, GORSE has a legitimate interest in

2.3.1. ensuring the safety of its premises and detecting and preventing any unlawful acts which may take place on its premises and

2.3.2. providing a safe and secure environment for pupils, staff and visitors, and investigating potential incidents.

2.4. In processing personal data through the medium of CCTV installations the organisation is carrying out a task in the public interest, namely the detection and prevention of unlawful acts as defined in the Data Protection Act 2018 (DPA) schedule 1 part 2 section 10.

The GORSE Academies Trust
c/o John Smeaton Academy, Smeaton Approach, Barwick Road, Leeds, LS15 8TA
T 0113 487 8888 | **E**: info@tgat.org.uk | **W** www.tgat.org.uk

3. CCTV Systems

3.1. GORSE uses a variety of CCTV systems across the academies. These systems consist of both analogue and IP cameras.

3.2. The cameras used on all systems consist of fixed cameras and movable cameras. These may also include cameras with the ability to zoom (a detailed inventory of cameras, specification and their view is recorded in the "CCTV Camera Inventory" at each site).

3.3. At the discretion of the principal, a trust establishment may also install 'replica' camera's – these do not have the functionality to record any data (image or audio) and are installed for the purposes of discouraging incidents.

3.4. Audio recording may be used in areas where it is deemed necessary to support the purpose of the system.

3.4.1. The audio feature should not be used to "Listen In" at any time unless it is required for safety and security of the staff, students or visitors. Details of all cameras with the ability to record audio will be recorded in the "CCTV Camera Inventory."

Fixed CCTV Camera Locations

3.5. CCTV cameras are located both inside and outside of the academy buildings:

3.6. All fixed CCTV cameras will be visible and in prominent areas.

3.7. Cameras may be located in classrooms and work areas. In these instances, staff, students and visitors will be informed and clear signage displayed.

3.8. Cameras will not be installed in areas where additional privacy is expected.

3.9. GORSE will do everything possible to ensure any area outside of the grounds of the trust establishment is not visible on the cameras or recordings, except for automated vehicle gates, to support with crime prevention and detection.

3.10. Signage will be displayed around the site ensuring staff, students and visitors are aware of the CCTV monitoring and how to find out more information.

4. Covert Recordings

4.1. The school may, in exceptional circumstances, set up covert monitoring where there is no less intrusive way of investigating. For example:

4.1.1. Where there is good cause to suspect that an illegal or unauthorised action(s), is taking place, or where there are grounds to suspect serious misconduct.

4.1.2. Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

4.2. Covert monitoring may take the following forms:

4.2.1. Cameras embedded in other equipment such as smoke detectors, glasses (including Google Glasses), watches, street furniture, PPE, pens, badges.

4.2.2. Cameras that are deliberately hidden to avoid detection.

The GORSE Academies Trust
c/o John Smeaton Academy, Smeaton Approach, Barwick Road, Leeds, LS15 8TA
T 0113 487 8888 | **E**: info@tgat.org.uk | **W** www.tgat.org.uk

4.2.3. Cameras that may not be obvious or obviously collecting footage such as drones, dash cams, Go Pros and similar small cameras that whilst not hidden are not obvious, body worn cams which may not be obvious to those being filmed.

4.2.4. Cameras used on mobile devices where their use is not obvious.

4.3. In these circumstances, authorisation must be obtained in writing from the DCEO or CEO and the Trust Board.

4.4. Covert monitoring must cease following the completion of an investigation.

5. Storage of Data

5.1. All data is stored directly on the Network Digital Video Recorder (NDVR), which is physically secure and accessible only to authorised members of staff.

5.2. Images are retained on the NDVR for no longer than 14 calendar days and no less than 5 calendar days. In the event of a Hard Disk or NDVR Failure, GORSE will attempt to recover footage, but the same data retention would apply.

5.3. If GORSE has reason to believe there is a significant threat to a site's security and may require recorded footage to be retained for longer than 14 calendar days, this will require approval from the CEO or Deputy CEO and must have a specified end date. Once this end date is reached all retained data beyond the 14 days must be removed in line with our data retention policy.

5.4. Any images required longer than individual establishment's retention period can be electronically held for review and must be deleted as soon as there is no longer basis to retain the data.

5.4.1. Where we are legally required to retain images and data for longer than the establishment's retention period for the purpose of evidential records, we shall do so in a secure manner.

6. Privacy

6.1. The installation or relocation of any camera will first go through an impact assessment to ensure full compliance with this policy.

6.2. An annual audit of camera locations, type of camera and purpose will be completed at each establishment, the records from this will be stored centrally. In the event of any in-year updates to the cameras at an establishment, the audit logs will be updated at the point of update. The responsibility for this will be held by the Principal and Director of Digital Strategy.

7. Access Management

7.1. Access to the CCTV recordings is controlled via assigned user accounts, which can only be used by designated members of staff.

7.2. The physical NDVR is kept securely locked away, preventing physical access.

8. Viewing of CCTV

8.1. Any viewing of footage is logged recording a minimum of date, time, person(s) accessing the footage, person supporting the viewing, reason for reviewing the footage, footage reviewed and a copy of the authorisation form.

8.2. Viewing of CCTV will require an access form to be completed by the member of staff needing to review footage and then approved by the Principal or Designated Senior Leaders prior to any footage being viewed **(Please see Appendix 1).** These forms must be retained in alignment with the GORSE Personal Data-Retention Policy.

8.2.1. If the principal is the requestor, the viewing of footage must be authorised by either the DCEO or CEO.

8.2.2. If CCTV is being used to support an allegation of staff misconduct, the Director of Human Resources must be contacted for support and guidance. This must also be approved by the CEO or DCEO in writing.

8.3. Viewing of the images should only be done for the purpose of items *1.2.1, 1.2.2, 1.2.3, 1.2.4.*

8.4. Viewing of recorded CCTV images shall take place in a restricted area. Other parties should not be allowed access when a viewing is taking place.

8.5. Recorded CCTV images shall not be retained by the reviewer once the viewing is concluded.

8.6. Routine access to the CCTV system by the following is authorised to enable them to carry out their daily duties.

8.6.1. IT Services – Maintenance of the physical system and software to ensure continued and reliable functionality.

8.6.2. Site Team – Access to cameras to maintain site security and daily functionality tests.

8.6.3. Contracted CCTV Monitoring Company – to monitor and maintain the security of the academy sites out of school hours.

8.7. **Viewing of live images**

8.7.1. Should only be done in line with item 3.1 or where there is suspicion that improper conduct may be carried out at a particular time.

8.7.2. Should only be in a controlled space with authorised personnel. Monitors should not be left on unattended.

8.7.3. The privacy of staff and students going about their normal legitimate business must be always respected.

8.7.4. Viewing of live images should only be used where there is an immediate safeguarding risk to students or staff on site.

8.7.4.1. The use of access control entry systems is excluded. Entry systems will be used by members of staff to authorise visitor

The GORSE Academies Trust
c/o John Smeaton Academy, Smeaton Approach, Barwick Road, Leeds, LS15 8TA
T 0113 487 8888 | **E**: info@tgat.org.uk | **W** www.tgat.org.uk

entry to the trust sites, no footage is recorded and is only live for the duration of the interaction between the visitor and the member of staff.

9. Subject Access Requests

9.1. Images will only be disclosed to data subjects as part of a Subject Access Request.

9.1.1. Images will only be supplied to the subject where either all subjects in the footage have consented to the disclosure, or the subject is the only person in the recording.

9.2. Images will not be disclosed where the disclosure will prejudice any criminal enquires.

9.3. All requests for disclosure will be recorded, where a request is declined the reason will also be recorded.

10. Third Party Requests

10.1. GORSE receives requests for the disclosure of CCTV footage from time to time from organisations such as the police. All employees receiving such a request shall pass the request to the Data Protection Lead.

10.2. GORSE shall assess each disclosure request on its merits and shall always exercise the highest degree of scrutiny and caution so as to ensure the privacy of the subjects who feature on the footage is not compromised. In assessing each request for disclosure, GORSE shall consider:

10.2.1. The purpose of the request, aim of the requestor and proposed use of the requested footage.

10.2.2. The lawful grounds for disclosure.

10.2.3. The rights of any individuals which may favour non-disclosure.

10.2.4. The necessity of the disclosure to further the requestors' purpose.

10.3. Requests for disclosure shall always be made in writing or written confirmation obtained to support verbal requests.

10.4. Requests from organisations such as the police are likely to be subject to the requesting organisation's policy, such as approved by senior management.

10.5. After considering all factors associated with the request, GORSE shall decide whether the footage should be disclosed and any terms relating to the disclosure.

10.6. GORSE shall maintain a register of disclosure requests.

11. Commissioning and Decommissioning

11.1. CCTV installations shall be subject to a commissioning process which shall include:

11.1.1. Checking that the installation is precisely as detailed in the Data Protection Impact Assessment (DPIA) or that a variation to the DPIA has been

approved. DPIA is a process used to identify, assess and minimise privacy risks before implementing a project that involves processing personal data.

11.1.2. Checking that cameras, cables, transmission equipment and data storage are tamper-proof

11.1.3. Collecting and retaining still images of the field of view of each camera for use as a future field of view reference point.

11.1.4. Checking and verifying that the access controls defined in the DPIR are in place and are effective.

11.1.5. Checking and verifying that the data retention policy defined in the DPIA is effective.

11.1.6. Ensuring appropriate signage is erected as detailed in the DPIA.

11.1.7. Checking that relevant information has been recorded on the CCTV location audit log.

10.2 When CCTV systems are no longer needed, they shall be subject to a decommissioning procedure that includes:

10.2.1 Removal of equipment.

10.2.2 Destruction of images.

10.2.3 Removal of signage.

12. Security of CCTV Images

12.1. GORSE shall ensure that all CCTV images are adequately protected from accidental or unlawful destruction, loss, or alternation, unauthorised disclosure or, or access to personal data transmitted, stored or otherwise processed through the implementation of technical and organisational controls and measures.

12.2. The systems used to collect, transmit, store and otherwise process CCTV footage are subject to the same high standards of IT security which run throughout the entirety of the organisation, including access controls, user authentication, anti-virus and malware software and penetration testing.

13. Data Subject Rights

13.1. As a controller of personal data all of the rights afforded to data subjects under the GDPR will apply to GORSE and the use of CCTV. In relation to this specific activity the Information Commissioner's Office (ICO) has provided some added clarification for some of the data subject's rights as follows:

13.2. Access rights.
Complying with access rights in relation to video surveillance could adversely affect the rights of other data subjects who are also identifiable

from the footage. Appropriate measures shall be used to protect these third parties. The organisation may also ask the data subject to specify reasonable timeframes to help with information searches. Reasonable timeframe should be sufficiently narrow to allow for the location of footage with a reasonable and proportionate search.

13.3. Right to erasure.
The ICO notes that blurring a picture with no retroactive ability to re-convert the picture into an identifiable image constitutes erasure in accordance with GDPR.

13.4. Right to object.
In case of video surveillance, this right could be exercised either prior to entering, during the time in, or after leaving the monitored area. This means that unless the controller has compelling legitimate grounds, monitoring an area where persons could be identified is only lawful if either (1) the controller is able to immediately stop the camera from processing personal data when requested, or (2) the monitored area restricted so that the controller can assure the approval from the data subject prior to entering.

14. Roles and Responsibilities

14.1. The Chief Executive Officer is responsible for ensuring that all GORSE data processing activities comply with the law and the best practices set out in its policies and procedures.

14.2. The Strategic Lead Officer and Director of Digital Strategy are responsible for defining work practices that are compliant with the law and best practices through establishing policies and procedures and ensuring that they are made available to all relevant people. They are responsible for monitoring all CCTV installations from their inception through their installation, operation and management.

14.3. The Director of Digital Strategy is responsible for ensuring that all information including video footage, still images, and audio recordings is captured, transmitted and stored securely.

14.4. Academies are responsible for

14.4.1. Undertaking DPIAs as required.

14.4.2. Ensuring the security of CCTV equipment under their responsibility and for complying with this policy and related documentation.

14.4.3. Ensuring the security of the information captured by CCTV equipment that they are responsible for.

14.4.4. Ensuring that the CCTV equipment they are responsible for is operating in compliance with this policy and related documents.

14.4.5. Ensuring that CCTV is only accessed or downloaded in accordance with GORSE policies and guidance.

14.5. All GORSE employees are responsible for reading, ensuring a full understanding of and complying with this policy and related procedures, and instructions. All employees are responsible for reporting to the Data Protection Lead any non-compliance that they are aware of or suspect.

15. Complaints

15.1. Complaints regarding the procedures laid down in this policy will follow that set out in the trust Complaint's Policy.

15.2. Complaints relating to information handling may be referred to the Information Commissioner.

The GORSE Academies Trust
c/o John Smeaton Academy, Smeaton Approach, Barwick Road, Leeds, LS15 8TA
T 0113 487 8888 | **E**: info@tgat.org.uk | **W** www.tgat.org.uk

The GORSE Academies Trust

Vehicle CCTV Policy

Designated Person:	Director of Digital Strategy/Strategic Lead Officer
Reviewed by:	Policy Committee
Date:	March 2026
Version:	1.5

The GORSE Academies Trust
c/o John Smeaton Academy, Smeaton Approach, Barwick Road, Leeds, LS15 8TA
T 0113 487 8888 | **E**: info@tgat.org.uk | **W** www.tgat.org.uk

CCTV POLICY (Dashcam)

1. Introduction

1.1. This policy is written in accordance with the General Data Protection Regulation ("GDPR") which came in to force on 25 May 2018 and the Data Protection Act 2018.

1.2. The GORSE Academies Trust ("GORSE") use Closed Circuit Television ("CCTV") across its academies for the following purposes:

1.2.1. To assist in providing a safe and secure environment for all students, staff and visitors.

1.2.2. To assist in the prevention and detection of crime and to assist law enforcement with investigations and criminal proceedings.

1.2.3. To assist in the prevention and detection of theft and criminal damage to all assets within GORSE.

1.2.4. All cameras will be used to support positive behaviour in all academies and provide visual evidence of any incident as well as crime prevention and detection.

1.2.4.1. Footage will also be used as evidence for any investigation relating to activity within the academy vehicles.

1.3. This policy is intended to provide protection against the misuse of Vehicle CCTV systems within GORSE.

1.4. The CCTV system will never be used as part of any staff performance appraisal.

2. Lawful Basis

2.1 As with all instances where personal data is processed there must be lawful basis for doing so in line with the GDPR.

2.2 GORSE will process personal data through the medium of CCTV installations where necessary to pursue its legitimate interests and to carry out tasks in the public interest.

2.3 In particular, GORSE has a legitimate interest in

2.3.1 ensuring the safety of its premises and detecting and preventing any unlawful acts which may take place on its premises and

2.3.2 providing a safe and secure environment for pupils, staff and visitors, and investigating potential incidents.

2.4 In processing personal data through the medium of CCTV installations the organisation is carrying out a task in the public interest, namely the detection and prevention of unlawful acts as defined in the Data Protection Act 2018 (DPA) schedule 1 part 2 section 10.

The GORSE Academies Trust
c/o John Smeaton Academy, Smeaton Approach, Barwick Road, Leeds, LS15 8TA
T 0113 487 8888 | **E**: info@tgat.org.uk | **W** www.tgat.org.uk

3. CCTV Systems

3.1. GORSE uses a variety of CCTV systems across academy vehicles. These systems all store media on local storage until it is transferred to the Trust network.

3.2. Audio recording where available may be enabled.

3.3. At the discretion of the principal, a trust establishment may also install 'replica' cameras – these do not have the functionality to record any data (image or audio) and are installed for the purposes of discouraging incidents.

4. Camera Locations

4.1. CCTV cameras are located inside the vehicles and can be setup to point into the passenger compartment and/or outside of the vehicle.

5. Covert Recordings

5.1. The establishment may, in exceptional circumstances, set up covert monitoring where there is no less intrusive way of investigating. For example:

5.1.1. Where there is good cause to suspect that an illegal or unauthorised action(s), is taking place, or where there are grounds to suspect serious misconduct.

5.1.2. Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

5.2. In these circumstances authorisation must be obtained in writing from the DCEO or CEO and the Trust Board.

5.3. Covert monitoring must cease following completion of an investigation.

5.4. Covert monitoring may take the following forms:

5.4.1. Cameras embedded in other equipment such as smoke detectors, glasses (including Google Glasses), watches, street furniture, PPE, pens, badges.

5.4.2. Cameras that are deliberately hidden to avoid detection.

5.4.3. Cameras that may not be obvious or obviously collecting footage such as drones, dash cams, Go Pros and similar small cameras that whilst not hidden are not obvious, body worn cams which may not be obvious to those being filmed.

5.4.4. Cameras used on mobile devices where their use is not obvious.

6. Storage of Data

6.1. All data is stored directly on the Dashcam (CCTV) temporarily until being transferred to the Trust network.

6.1.1. Data should be deleted from the Dashcam once it is securely stored on the Trust network.

6.1.2. All data should be transferred to the trust network within 3 working days of it being recorded.

6.2. Images are retained securely on the trust network for a period no longer than 14 calendar days but no less than 5 calendar days.

6.3. Any images required longer than individual establishment's retention period can be electronically held for review and must be deleted as soon as there is no longer basis to retain the data.

6.3.1. Where we are legally required to retain images and data for longer than the establishment's retention period for the purpose of evidential records, we shall do so in a secure manner.

6.3.2. In the event of a vehicle being involved in an accident, we will retain any dashcam footage for insurance purposes.

7. Privacy

7.1. Each camera is subject to a regular review to ensure it is still fulfilling its intended purpose.

8. Access Management

8.1. Access to the CCTV recordings stored on the trust network are controlled via assigned user accounts, which can only be used by designated members of staff.

8.2. The physical camera and storage card are kept secure and locked away, preventing physical access when it is not in use.

9. Viewing of CCTV

9.1. Any viewing of footage is logged recording a minimum of date, time, person(s) accessing the footage, person supporting the viewing, reason for reviewing the footage, footage reviewed and a copy of the authorisation form.

9.2. Viewing of CCTV will require an access form to be completed by the member of staff needing to review footage and then approved by the Principal or Designated Senior Leaders prior to any footage being viewed **(Please see Appendix 1).** These forms must be retained in alignment with the GORSE Personal Data-Retention Policy.

9.2.1. If the principal is the requestor, the viewing of footage must be authorised by either the Designated Senior Leaders at the establishment, DCEO or CEO.

9.3. Viewing of the images should only be done for the purpose of items *1.2.1, 1.2.2, 1.2.3, 1.2.4 and 1.2.4.1*

9.4. Viewing of recorded CCTV images shall take place in a restricted area. Other parties should not be allowed access when a viewing is taking place.

9.5. Recorded CCTV images shall not be retained by the reviewer once the viewing is concluded.

9.6. Routine access to the vehicle CCTV system and trust network by the following is authorised to enable them to carry out their daily duties.

9.6.1. IT Services – Maintenance of the physical device and software to ensure continued and reliable functionality.

10. Subject Access Requests

10.1. Images will only be disclosed as part of a subject access request.

10.1.1. Images will only be supplied to the subject where either all subjects in the footage have consented to the disclosure, or the subject is the only person in the recording.

10.2. Images will not be disclosed where the disclosure will prejudice any criminal enquires.

10.3. All requests for disclosure will be recorded, where a request is declined the reason will also be recorded.

11. Third Party Requests

11.1 GORSE received requests for the disclosure of CCTV footage from time to time from organisations such as the police. All employees receiving such a request shall pass the request to the Data Protection Lead.

11.2 GORSE shall assess each disclosure request on its merits and shall always exercise the highest degree of scrutiny and caution so as to ensure the privacy of the subjects who feature on the footage is not compromised. In assessing each request for disclosure, GORSE shall consider:

11.2.1. The purpose of the request, aim of the requestor and proposed use of the requested footage.

11.2.2. The lawful grounds for disclosure.

11.2.3. The rights of any individuals which may favour non-disclosure.

11.2.4. The necessity of the disclosure to further the requestors' purpose.

11.3. Requests for disclosure shall always be made in writing or written confirmation obtained to support verbal requests.

11.4. Requests from organisations such as the police are likely to be subject to the requesting organisation's policy, such as approved by senior management.

11.5. After considering all factors associated with the request, GORSE shall decide whether the footage should be disclosed and any terms relating to the disclosure.

11.6. GORSE shall maintain a register of disclosure requests.

12. Complaints

12.3. Complaints regarding the procedures laid down in this policy will follow that set out in the trust Complaint's Policy.

12.4. Complaints relating to information handling may be referred to the Information Commissioner.

The GORSE Academies Trust

Call Recording Policy

Designated Person:	Director of Digital Strategy/Strategic Lead Officer
Reviewed by:	Policy Committee
Date:	March 2026
Version:	1.5

The GORSE Academies Trust
c/o John Smeaton Academy, Smeaton Approach, Barwick Road, Leeds, LS15 8TA
T 0113 487 8888 | **E**: info@tgat.org.uk | **W** www.tgat.org.uk

CALL RECORDING POLICY

1. Introduction

1.1. This policy is written in accordance with the General Data Protection Regulation ("GDPR") which came in to force on 25 May 2018 and the Data Protection Act 2018.

1.2. The GORSE Academies Trust ("GORSE") may use Call-Recording software/hardware to assist in the resolution of enquiries from parents/carers.

1.3. Recordings will be used for any investigation relating to interaction between parents/carers and trust establishment staff.

1.4. This policy is intended to provide protection against the misuse of call recording software/hardware.

1.5. The contents of specific calls will not be used as part of any staff performance appraisal. Metrics from the call-management solution (for example, the volume of calls handled by staff members) may be used for the improvement of service levels.

2. Recording Systems

2.1. GORSE uses a variety of recording systems, these systems transfer the recording to the secure academy network.

2.2. Systems are integrated to the trust establishment's telephony services and maintained by the GORSE IT team.

2.3. Inbound callers must be advised that their call may be recorded in line with data regulations. This is via an automated message played to the caller prior to the call being connected.

3. Storage of Data

3.1. All data is stored on the secure trust establishment's network.

3.2. A recording is retained on the on the Trust network for a period no longer than 14 calendar days but no less than 5 calendar days.

3.3. Any recording required longer than individual Trust establishment's retention period can be electronically held for review and must be deleted as soon as there is no longer basis to retain the data.

3.4. When a recording is stored, for longer than the 14-day maximum period, approval must be sought from a senior member of staff for this to happen.

3.4.1. Where we are legally required to retain data for longer than the trust establishment's retention period for the purpose of evidential records, we shall do so in a secure manner.

4. Access Management

4.1. Access to the recordings stored on the Trust network are controlled via assigned user accounts which can only be used by designated members of staff.

The GORSE Academies Trust
c/o John Smeaton Academy, Smeaton Approach, Barwick Road, Leeds, LS15 8TA
T 0113 487 8888 | **E**: info@tgat.org.uk | **W** www.tgat.org.uk

5. Accessing recordings

5.1. Any accessing of recording is logged recording a minimum of date, time, person(s) accessing the recording, person supporting the access, reason for reviewing the recording, the recording reviewed and a copy of the authorisation form.

5.2. Access to recordings will require an access form to be completed by the member of staff needing to review the recording and then approved by the principal or Designated Senior Leaders prior to any recording being accessed **(please see Appendix 2).** These forms must be retained in alignment with the GORSE Personal Data-Retention Policy.

5.2.1. If the principal is the requestor, the access of the recording must be authorised by either the DCEO or CEO.

5.3. Accessing of the data within call-recording archives should only be done for the purpose of items 1.2 & 1.3

5.4. Routine access to the recording solution and trust network by the following is authorised to enable them to carry out their daily duties.

5.4.1. IT Services – Maintenance of the physical device and software to ensure continued and reliable functionality.

6. Disclosure

6.1. Data will only be disclosed as part of a Subject Access Request.

6.1.1. Recordings will only be supplied to the subject where all subjects in the recording have consented to the disclosure.

6.2. Recordings will not be disclosed where the disclosure will prejudice any criminal enquires.

6.3. All requests for disclosure will be recorded, where a request is declined the reason will also be recorded.

7. Third Party Requests

7.1 GORSE receives requests for the disclosure of recordings from time to time from organisations such as the police. All employees receiving such a request shall pass the request to the Data Protection Lead.

7.2 GORSE shall assess each disclosure request on its merits and shall always exercise the highest degree of scrutiny and caution so as to ensure the privacy of the subjects who feature on the recording is not compromised. In assessing each request for disclosure, GORSE shall consider:

7.2.1. The purpose of the request, aim of the requestor and proposed us of the requested recording.

7.2.2. The lawful grounds for disclosure.

7.2.3. The rights of any individuals which may favour non-disclosure.

7.2.4. The necessity of the disclosure to further the requestors' purpose.

The GORSE Academies Trust
c/o John Smeaton Academy, Smeaton Approach, Barwick Road, Leeds, LS15 8TA
T 0113 487 8888 | **E**: info@tgat.org.uk | **W** www.tgat.org.uk

7.3 Requests for disclosure shall always be made in writing or written confirmation obtained to support verbal requests.

7.4 Requests from organisations such as the police are likely to be subject to the requesting organisation's policy, such as approved by senior management.

7.5 After considering all factors associated with the request, GORSE shall decide whether the recording should be disclosed and any terms relating to the disclosure.

7.6 GORSE shall maintain a register of disclosure requests.

8. Complaints

8.1. Complaints regarding the procedures laid down in this policy will follow that set out in the trust Complaint's Policy.

8.2. Complaints relating to information handling may be referred to the Information Commissioner's Office.

Document control:

Reason for version change:	Cycle review/refresh	Version number:	1.5
Date of Approval:	March 2026	Approved by:	Policy Committee
Target Audience:	• Principals and Senior leaders • GORSE Executive • Operations Managers, Business Managers and Site Teams • GORSE IT Teams • GORSE Websites	Date issued:	March 2026

The GORSE Academies Trust
c/o John Smeaton Academy, Smeaton Approach, Barwick Road, Leeds, LS15 8TA
T 0113 487 8888 | **E**: info@tgat.org.uk | **W** www.tgat.org.uk

APPENDIX 1

Request to View CCTV

This form must be completed, and authorisation provided prior to any CCTV footage being reviewed.

Requestors Name		Today's Date	
Requestors Job Title		Academy Name	

Details of Footage to be viewed			
Date of footage to be viewed		Time of footage to be viewed	
Location of footage to be viewed (Include details of all locations that need to be reviewed as part of this request)			
Reason for request (Please include any reference numbers connected to this request)			
Requestors signature			
Approved by			

The GORSE Academies Trust
c/o John Smeaton Academy, Smeaton Approach, Barwick Road, Leeds, LS15 8TA
T 0113 487 8888 | **E**: info@tgat.org.uk | **W** www.tgat.org.uk

(Include Job Title)	
Approvers Signature	
Date of Approval	

Form Reference: CCTV Request and Authorisation Log v1

The GORSE Academies Trust
c/o John Smeaton Academy, Smeaton Approach, Barwick Road, Leeds, LS15 8TA
T 0113 487 8888 | **E**: info@tgat.org.uk | **W** www.tgat.org.uk

Record of CCTV Viewing

This form must be completed, following the viewing of all CCTV footage

Details of Approved Request			
Requestors Name		Request date	
Approved by		Approved date	

Details of Review			
Date CCTV Reviewed		Time CCTV Reviewed	
Persons present during review. (Include Full names and reason for their presence)			
CCTV shared with other parties. (Include date shared, who by, who with, and purpose for sharing the footage)			

Details of Footage Viewed			
Date of footage viewed		Time of footage viewed	
Location of footage viewed (Include camera numbers and location names)			
Findings from the viewing. (detail the findings for each camera viewed, where nothing was found make this clear)			

The GORSE Academies Trust
c/o John Smeaton Academy, Smeaton Approach, Barwick Road, Leeds, LS15 8TA
T 0113 487 8888 | **E**: info@tgat.org.uk | **W** www.tgat.org.uk

Site Team - Viewing Sign Off			
Signature (Include Job Title)		Name and Position	

Form Reference: CCTV Access Log v1

The GORSE Academies Trust
c/o John Smeaton Academy, Smeaton Approach, Barwick Road, Leeds, LS15 8TA
T 0113 487 8888 | **E**: info@tgat.org.uk | **W** www.tgat.org.uk

Record of CCTV Maintenance

This form must be completed, at the time of any Maintenance or function checks where the CCTV system is either accessed or cameras adjusted

Details of Review			
Date CCTV maintenance		Time CCTV maintenance	
Persons involved in the CCTV maintenance. (Include Full names and reason for their presence)			
Details of Footage Viewed			
Details of all maintenance carried out. (Include details of any cameras that are checked, any adjustments to cameras and the reasons for these changes)			
Findings from the maintenance. (detail any findings or further actions that are required)			
Maintenance Sign Off			
Signature of person leading maintenance		Name and Position	

Form Reference: CCTV Maintenance Log v1

The GORSE Academies Trust
c/o John Smeaton Academy, Smeaton Approach, Barwick Road, Leeds, LS15 8TA
T 0113 487 8888 | **E**: info@tgat.org.uk | **W** www.tgat.org.uk

APPENDIX 2

Request to Access: Call-Recording

This form must be completed, and authorisation provided prior to any call recording being reviewed.

Requestor's Name		Today's Date	
Requestor's Job Title		Trust Establishment Name	

Details of recording to be accessed			
Date of recording to be accessed		Time of recording to be accessed	
Reason for request (Please include any reference numbers connected to this request)			
Requestor's signature			
Approved by (Include Job Title)			
Approver's Signature			
Date of Approval			

Form Reference: Call Recording Request and Authorisation Log v1

The GORSE Academies Trust
c/o John Smeaton Academy, Smeaton Approach, Barwick Road, Leeds, LS15 8TA
T 0113 487 8888 | **E**: info@tgat.org.uk | **W** www.tgat.org.uk

Record of recording access

This form must be completed, following the review of any accessed recording

Details of Approved Request			
Requestor's Name		Request date	
Approved by		Approved date	

Details of Review			
Date recording accessed		Time recording accessed	
Persons present during review. (Include full names, job titles and reason for their presence)			
Recording shared with other parties. (Include date shared, who by, who with, and purpose for sharing the recording)			

Details of Review			
Date of recording accessed		Time of recording accessed	
Findings from the access.			

The GORSE Academies Trust
c/o John Smeaton Academy, Smeaton Approach, Barwick Road, Leeds, LS15 8TA
T 0113 487 8888 | **E**: info@tgat.org.uk | **W** www.tgat.org.uk

Access Sign Off			
Signature (Include Job Title)		Name and Position	

Form Reference: Call Recording Access Log v1

The GORSE Academies Trust
c/o John Smeaton Academy, Smeaton Approach, Barwick Road, Leeds, LS15 8TA
T 0113 487 8888 | **E**: info@tgat.org.uk | **W** www.tgat.org.uk

Record of Call-Recording Maintenance

This form must be completed, at the time of any Maintenance or function checks where the Call-Recording system is accessed or adjusted

Details of Review			
Date Call Recording maintenance		Time Call Recording maintenance	
Persons involved in the Call Recording maintenance. (Include full names, job titles and reason for their presence)			
Details of maintenance			
Details of all maintenance carried out.			
Findings from the maintenance. (detail any findings or further actions that are required)			
Maintenance Sign Off			
Signature of person leading maintenance		Name and Position	

Form Reference: Call Recording Maintenance Log v1

The GORSE Academies Trust
c/o John Smeaton Academy, Smeaton Approach, Barwick Road, Leeds, LS15 8TA
T 0113 487 8888 | **E**: info@tgat.org.uk | **W** www.tgat.org.uk