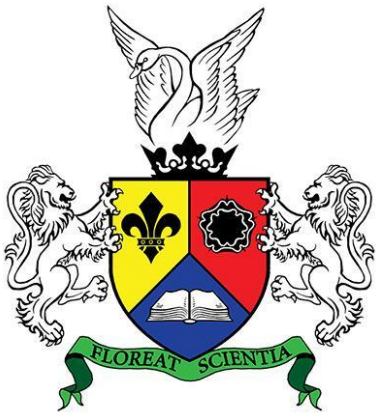


CCTV
Code of Practice:
Fakenham Academy

Version Control Document

Date	Version No.	Reason for Change	Author
August 2015	1.0	Review by D.Bowie	Dawn Clarke
October 2018	1.1	Review by Information Compliance	Information
		Team	Compliance
			Team
November 2018	1.2	Review by FAN	Neil Jary
April 2019	1.3	Proposal/install of new Cameras	Neil Jary
July 2019	1.4	Proposal of new Cameras	Neil Jary
Sep 2019	1.5	New camera installs and location	Neil jary
Jan 2020	1.6	Amendment suggestion	
Feb 2020	1.7	new camera install	Neil Jary
Sep 2020	1.8	edit for new Academy trust	Neil Jary
April 2021	1.9	Edit for removal of NES and previous branding plus staff changes	Neil Jary
September 2021	2	review and additions for new trust	Neil Jary
March 2022	2.1	review and minor changes	neil jary
March 2022	2.2	added CLA as authorised	Neil Jary
September 2023	2.3	Addition of cameras	Neil Jary

This document is accurate at the time of Introduction, requests from students/parents/staff due to any issues that may arise, may result in this document being updated, and listed as the next sequential version.

Contents

1. Introduction

This Closed Circuit Television (CCTV) Code of Practice is established under the Sapientia Data Protection Policy and is to be read in conjunction with that policy. Certain elements of the policy have been repeated in full in the Code of Practice because of the importance of the message.

2. Aims & Objectives

This Code of Practice aims to ensure that the CCTV systems installed and operated by Fakenham Academy, comply with the law and that the scope, purpose and use of the systems are clearly defined.

3. Scope

This Code of Practice applies to Vivotek CCTV installed at Fakenham Academy, and to all employees permanent or temporary of Sapientia and includes any agency, or visiting professionals employed to provide services on their behalf.

4. Operational Arrangements

4.1 Ownership

The CCTV system, all recorded material and copyright are owned by Fakenham Academy.

The CCTV Manager of the system is Headteacher and OPS Manager

The Data Controller is the Headteacher.

*The Data Processor are The 'Deputy Headteachers and OPS Manager, assisted by The Network Manager.

4.2 Principles of Operation

The principles that govern the operation of the CCTV system are stated in full in the CCTV Guidance Note (Appendix 1) and summarised below:

- The CCTV system will be operated fairly and lawfully and only for the purposes authorised by the organisation as notified to the Information Commissioner's Office.
- There will be transparency and accountability in how the CCTV system is operated.
- The CCTV system will be operated with due regard for the privacy of the individual, including camera siting, access to and disclosure of images, and the retention of recorded footage.
- Appropriate technical and procedural security measures will be employed to protect the footage record from unauthorised access.

- Any changes to the purpose for which the CCTV system is operated will require the prior approval of the Headteacher

4.3 Purpose of the CCTV System

A Data Protection Impact Assessment (DPIA) has been conducted and has determined the purposes for the operation of the CCTV system.

The system is intended to provide an increased level of security in the organisation's environment for the benefit of those who study, work or visit the campus.

The CCTV system will only be used to respond to the following key objectives which will be subject to annual assessment.

- To detect, prevent or reduce the incidence of crime
- To prevent and respond effectively to all forms of harassment and public disorder
- To reduce the fear of crime
- To create a safer community
- To gather evidence by a fair and accountable method
- To provide emergency services assistance
- To provide assistance for internal investigations/disciplinary hearings within the institution for the purpose of safety and security of all campus users and their property

With regard to internal investigations/disciplinary hearings, CCTV images will be used only when the alleged conduct is classed as 'gross misconduct' according to the organisation's employee and student conduct policies AND the alleged conduct is deemed to have compromised the safety and security of individuals or property.
CCTV systems will NOT be used to monitor the performance of employees.

4.4 System Detail

The CCTV system consists of 31 Vivotek (0 to be authorised) cameras situated on the organisation's property both in buildings and externally which continuously record activities in that area.
The cameras are linked to Vivotek CCTV system server which is located in the secure server room at the Academy

Location of Cameras:

1. Main entrance
2. School Bungalow
3. T01 IT Suite
4. Front of Tech Block
5. Withdrawal 1-3
6. Withdrawal 4-6
7. Withdrawal L shaped room
8. Withdrawal back room
9. KS3 Confab
10. Outside deputy Headteacher office (Foyer)
11. KS4 Confab
12. Dining room servery
13. Perowne building Boys Toilets entrance
14. Perowne building eating area Art end
15. Perowne building eating area Science end
16. Perowne building facing field
17. Reception
18. Lancastrian Block Front
19. MUGA

20. Back gate
21. Front pedestrian gate (not installed as of 2/11/18)
22. Canteen Serving Area
23. L17 IT room
24. L27 IT Room
25. Canteen area (reception end)
26. T13 Music Room
27. T05 IT room
28. Withdrawal facing Bike Shed
29. Tech Department Prep Room
30. Tech department rear door to prep room and wood store and back gate
31. Girls Confab Toilets
32. Boys Confab Toilets

Sound is currently only recorded in the Withdrawal unit due to the special safeguarding issues raised within that environment.

4.5 Maintenance

The Organisation has full responsibility to ensure that the CCTV cameras and system equipment are kept in full and appropriate working order, with correct camera locations, dates and times shown on the system and on footage.

The Maintenance program includes a program of cleaning and housekeeping of the system as well as 24/7 call-out for breakdown and replacement camera cover.
It is the Organisations responsibility to ensure that the quality of images produced are enough to meet the purposes of the CCTV system.

4.6 Installation and Signage

All cameras are located in prominent positions to ensure they only capture images to meet the key objectives outlined at 4.3 above and an assessment is carried out prior to installation to ensure that cameras are located appropriately. The assessment was conducted with senior leaders and IT support services to ensure that locations chosen for CCTV installation were feasible for IT to reach, but also necessary to meet the objectives of 4.3 above.
Cameras are installed in such a manner as not to overlook private domestic areas outside the premises perimeter.
Cameras are not hidden from view and signs are prominently displayed on the external perimeter of the premises in the locality of the cameras. The signs indicate:

- The presence of monitoring and recording
- The purpose of the System
- The ownership of the System
- Contact point address details

Signs are in place at relevant points inside the premises to advise students, staff and visitors that CCTV cameras are in use. In particular signs must be in place when cameras are sited in locations where people might reasonably expect privacy, e.g. changing rooms, entrance to toilets; or when the cameras are very discreet.

4.7 Staff CCTV Operator Training

Staff using the CCTV System will be given full training on its use, covering the CCTV Guidance Note and this Code of practice.

4.8 Access to Live Footage and Recordings

4.8.1 The CCTV Manager is responsible for:

- Ensuring that any requests are consistent with the purposes for use of the CCTV system, using the checklist at Appendix A;
- That all requests are logged, including those where access is refused
- Where viewing/disclosure is granted, the log includes a record of the date/time and nature of the footage, including the data subjects involved and the reason for the request.

4.8.2 Access to Live Footage.

Monitoring of Live Footage

- Monitoring of live footage as a matter of routine should be limited to areas such as entrances to the site. Where live footage from CCTV cameras is streamed to screens which are monitored, full details will be entered below to cover the siting of the screens, which cameras are monitored and the postholders who have been designated and trained to carry out the monitoring.

- Withdrawal Unit: there are 4 cameras located in this building for the safeguarding of teaching staff and pupils; Live footage will be monitored by the member of staff in charge of the Withdrawal unit at the given time. Due to the nature of the environment sound will be recorded by these cameras. Relevant signs will be in place stating this fact. Staff who operate in this area have been consulted regarding the recording of sound.

The viewing of live footage should be limited only to incidents of a serious nature relating to crime, in particular incidents of significant disorder or where students or staff are at risk of harm. Such incidents will be rare.

Live footage may be viewed at any time by the police for the purpose of preventing crime and/or the identification and apprehension of offenders at the time the incident is occurring. However, the police do not have a general power to record images or to re-position or focus the cameras directly for the purpose of criminal investigation. If police wish to record live footage, or re-position/focus a camera directly they will need to provide a written form of authority under the Regulation of Investigatory Powers Act (RIPA). The only exception is where there is a live incident occurring and it is not practicable for RIPA authorisation to be sought.

4.8.3 Access to Recorded Footage

Where staff are contracted to provide security services on the premises, designated staff will have direct access to CCTV recordings, for operational purposes and in accordance with the stated purposes of the system only.

In all other circumstances only the CCTV Manager, Assistants and the Headteacher will have the authority to view recorded footage. Footage can be viewed only for the purposes described at 4.3 above. ALL viewing of footage will be logged.

Where a member of Sapientia Group staff requests to view recorded footage, the CCTV Manager or Headteacher will be required to authorise the viewing.

4.8.4 Disclosure of Recorded Material

A copy of recorded footage will be disclosed only for the purposes at 4.3 above and only where an assessment using the checklist at Appendix A has been made that the disclosure is necessary for the purpose. Disclosure of recorded footage to an external third party should be very rare.

4.8.5 Release of images for the Prevention and Detection of Crime

Where it is believed a crime has occurred and the organisation has initiated contact with the police, and there is a reasonable belief that the CCTV recorded materials will be of assistance in the police investigation, the CCTV Manager or the Headteacher can authorise the pro-active release of recorded footage.

Where the police or other official body with investigation/prosecuting powers approach the organisation and request access to CCTV footage they shall be asked to provide a Request to external organisation for the disclosure of personal data form or similar document confirming that the information is necessary for either the prevention of crime of the apprehension or prosecution of offenders, or matters of national security. Requests of this nature rely in the following legislation: Under Schedule 2 Part 1 Paragraph 2 of the DPA 2018 and GDPR Article 6(1)(d).The CCTV Manager will ensure such requests are assessed and logged.

4.8.6 Subject Access Request

A person is entitled to request access to their personal data, which can include CCTV footage. Such requests will be forwarded to the Headteacher for processing.

The applicant will be required to provide a reasonable timeframe and location of when/where they believe the recording to have occurred and a full-face photograph for identification purposes. The CCTV Manager will be responsible for arranging the searches and extraction of the relevant footage, in liaison with the Headteacher. Where the footage shows identifiable third parties, a decision will need to be made whether it is reasonable to provide the footage to the applicant, or whether steps may need to be taken to obscure the images of third parties. The technicalities of this will need to be addressed, bearing in mind a response to a subject access request is to be made within 1 calendar month.

Where agreed by the applicant, arrangements may be made for the applicant to view the relevant footage on site. However, in most cases a copy will be provided.

4.8.7 Freedom of Information Requests

Any person can make a request for information held by Fakenham Academy, which can include CCTV images. As for subject access requests, steps should be taken immediately to preserve the recorded images for the relevant period whilst full assessment of the request takes place with the advice of the Headteacher.

4.9 Retention of Recorded Material and Disposal

CCTV Recordings are recorded to Server hard drive and retained for 14 days unless an incident is recorded which requires further investigation either by senior management, the police or another external body with prosecuting powers.

Server storage space and costs plus the HD quality of footage from the camera system limit the viability of storing footage for much longer than 14 days; and given the relatively quick involvement of safeguarding and pastoral teams on site, footage to be kept would be requested well within a 14 day period and stored separately when connected to an incident.

Where recordings are extracted for internal issues of safety etc, they are stored on a Secure folder storage on the CCTV server and the only copies are held by the CCTV Manager and the person nominated by the Headteacher to carry out the internal review/investigation. This footage will be stored for a time limit that is dictated by the incident and the notes of that time period will be added to the CCTV footage record of the incident in question. Once the incident is dealt with, said footage will be destroyed. Maximum time limit for this would be 14 days unless footage is being externally requested by Police, safeguarding or other external source where data is stored offsite.

All media on which recordings were made that are no longer required will be shredded (in the case of CD/DVD discs) and the appropriate details entered in the CCTV Log-Disclosure of Recorded Material form which is accessed via secure Onedrive.

4.10 Administration

A Google form and spreadsheet is kept with all relevant access to the system; this is dated and signed (digitally) and kept on a secure cloud based Google folder; accessible by Headteacher, CCTV manager and assistant and staff for technical purposes.

4.11 Disclosure of Recorded Material

Internal Requests for Information

Internal requests for access to CCTV footage must be logged by the CCTV Manager, including the purpose for the request for access, and full details of the footage. The CCTV Manager should verify any request with a member of senior management.

Police Request for Information

The Request for CCTV footage Form (appendix 2) is used for request by police for footage. It will also be noted in the document created by that form (appendix 3) if footage is copied to DVD/USB device and when that footage will be destroyed. This will be the responsibility of the CCTV manager or assistant to ensure that data is correct at the time of request and that destruction is carried out.

Police Requests for access. This form is also used to record the destruction of recorded DVDs. Each section of the form must be completed at the relevant stage. (Appendix 2 and 3)

5. Breaches of the Code and Complaints

A copy of this Code of Practice will be made available to anyone requesting it. Any complaint concerning misuse of the system will be treated seriously and investigated by the CCTV Manager or nominee with advice from the Headteacher as appropriate.

The CCTV Manager or nominee will ensure that every complaint is acknowledged in writing within seven working days, which will include advice to the complainant of the enquiry procedure to be undertaken.

Breaches of this Code of Practice shall be dealt with in accordance with the appropriate disciplinary policy. Serious breach of the Code may result in criminal liability on behalf of the individual which may also be considered as gross misconduct.

Where appropriate, the police will be asked to investigate any matter relating to the CCTV system which is deemed to be of a criminal nature.

6. Contact

- CCTV Manager –Headteacher, Fakenham Academy 01328 857005
- CCTV/Security - IT Manager, Fakenham Academy 01328 857027

Appendix 1 – Data Protection Impact Assessment

A: Data Protection Impact Assessment (DPIA) Screening

It is important that the Group actively manages the risks around processing of personal data. Part of this management is the completion of Data Protection Impact Assessments (DPIAs). These assessments encourage people to look carefully at what they are doing with personal data, why they are doing it, the risks involved and controlling those risks to an acceptable level.

Before you complete a DPIA, let's identify if one is required. If you answer YES to any of the questions below, please proceed to part B.

Screening Questions (please answer ALL questions)	YES/NO

Does your proposal involve the processing of any of the following?

- CCTV

- Biometrics (e.g. fingerprint, retina scan)
- ‘High Risk data’ (see Annex A)

Will the project/activity involve the collection of new personal information about individuals? (i.e. types of data the institution has not previously recorded, or about a group of individuals not previously involved)

Yes; CCTV footage will be recorded

Will the project/activity require individuals to provide information about themselves? (i.e. will individuals have a **choice** of whether or not to provide the information?)

No

Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information? (This will include partnership arrangements with another organisation, requests from local authority/government agencies, providing data for a software service hosted online or by a third party)

No

Does the project/activity involve you using new technology that might be perceived as being privacy intrusive? (For example the use of biometrics, moving an existing process online, filming/recording individuals)

Yes; CCTV cameras will be located throughout the Academy site

Will the project/activity involve using data to make automated decisions or undertake profiling about individuals in ways that have a significant impact on them? (For example, using performance data to decide on salary increases)

No

Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? (For example, ‘special category data’ such as health records, criminal records or other information that people would consider to be private?)

No

Is data being transferred outside of Europe?

No

B: Data Protection Impact Assessment (DPIA) Form

This form helps gather initial information internally, and from third party data processors with whom the organisation may need to share personal data for the fulfilment of a service. The form should be completed prior to a change in personal data processing OR the purchase of the service the involves the sharing of personal data. The form can also be used to assess a current service.

All sections can be expanded as required and the list of questions is not exhaustive. Responses may prompt additional enquiries.

Document control information	
Service name:	Vivotek CCTV system
Date:	1/11/2018
Author(s):	Neil Jary, Cathrine Lane
Service Contact point (for future privacy concerns)	01328 857027

Step 1: Identify the need for a DPIA

Explain broadly what the project aims to achieve and what type of personal data processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal.

What does the project/service aim to achieve?

The purpose of using CCTV is to protect staff, students, visitors and property from the actions of individuals. These actions may not necessarily be criminal offences but will have a negative impact on teaching, learning and employees' working environment. Being a large secondary school with over 800 students and a very disjointed set of buildings, monitoring behaviour using staff alone can be a challenge. CCTV images are recorded so that they can be used to establish who committed an offence. The CCTV recordings are used alongside traditional ways of investigating such as obtaining witness statements

What are the expected benefits to the organisation?

To create a comfortable and safe learning and working environment.

What benefits to individuals and other parties are expected, if applicable?

Students feel safer and more confident walking around site as they know that instances or poor behaviour whilst not tolerated, can also be seen, even if there is not a member of staff present. Staff feel safer having a second set of eyes in the event of an allegation or incident.

Why was the need for a DPIA identified? (Refer to the Screening Questions)

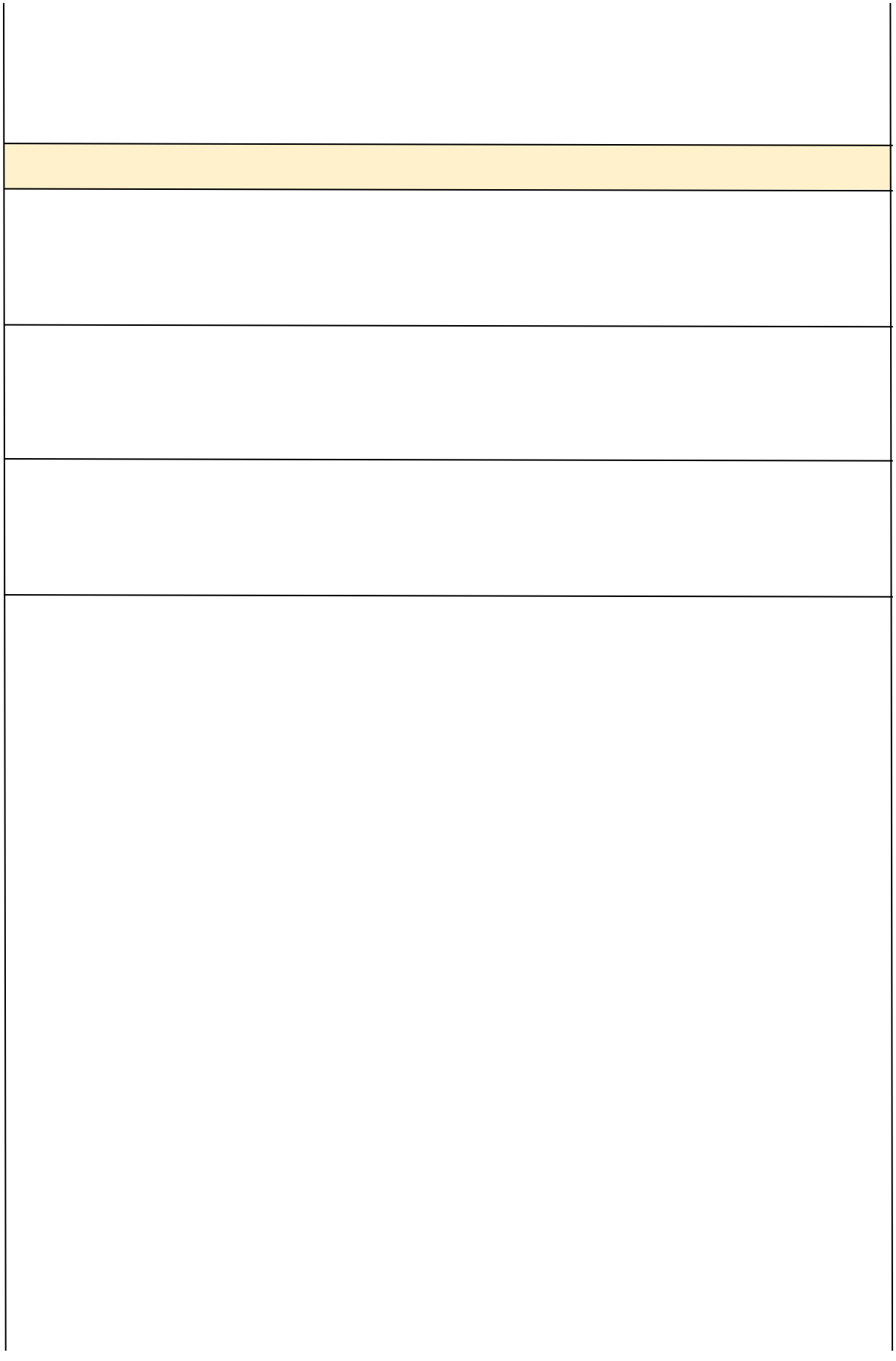
Integration of CCTV system throughout academy site.

What alternative solutions to the proposed project/service have been considered?

On location staffing and lunchtime supervisors

Why were these alternatives deemed unsuitable?

The need for staff at various locations throughout the site and, with regard to in classroom systems (withdrawal), the requirement for safeguarding at all times for staff and pupils. Staffing levels and workload of the Academy; and the use of lunchtime mentors and supervisors requires an added measure of security when dealing with issues that might arise. The CCTV system will also allow full tracking of an incident if it moves throughout various areas of the school.



Step 2: Describe the processing

Will the personal information be new information as opposed to existing information used in new ways?
It will be new information

Who are the Data Subjects? (Students, Staff, Contractors, Visitors, groups of these etc)
All persons located at the Fakenham Academy site on a daily basis or visiting the site.

How many Data Subject records will be processed? (How many individual's records per year – is this cumulative?)
All persons located at Fakenham Academy either on a daily basis or visiting the site.

What types of data will be processed? (Name, Identifier, Address, Ethnicity, Images etc.)

Video footage

Are all these data types required for the project/service?

yes

Is the data adequate, relevant and not excessive? Can you minimise the amount of data being provided and still achieve the same outcome?

Data will be kept to the minimum unless specific circumstances arise that require additional data recording (sound)

Is there a statutory requirement to process this data? (Please quote the regulations if 'yes')

No

How will you help to support the rights of the Data Subject(s)? (Right to access, right to be forgotten etc.)

The data subject will be made aware of their rights under data protection legislation via the relevant Academy privacy notices

---

What is the lawful basis for processing – Is the consent of the Data Subject required?

No consent is required but Fakenham Academy clearly inform data subjects regarding recording via appropriate signage, privacy notices and their CCTV Code of Practice document.

Will the project/service involve new elements that require the organisation's Privacy Notice to be amended? If yes, please identify the changes that need to be made to the Privacy Notice.
Yes; privacy notice will be amended to show relevant usage of CCTV footage and camera locations.

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Who should be consulted **internally** to help identify and address privacy risks? *The Information Compliance Team should be consulted in all cases.*

(Roles / Groups):

- Student Representative(s) ☐
- Staff Representative(s) ☐
- Governors ☐
- Other: Please specify ☐

How will you consult internally?

All of the above groups highlighted have been consulted on the implementation of this system

Who should be consulted **externally** to help identify and address privacy risks? *The Information Compliance Team should be consulted in all cases.*

(Roles / Groups):

- Service Providers ☐
- Contractors ☐
- Other: Please specify ☐

How will you consult externally?

No service providers or contractors are affected by the implementation of this system.

Step 4: Identify and assess risks

Based on your responses to the screening questions (document A) and section 3 above, identify the key privacy risks and the associated compliance and organisational risks. Depending on the scale of your project, you might also record this information on a more formal risk register. *Some example risks are listed at Annex B*.

Privacy issue	Risk to individuals	Likelihood of harm *Remote, possible or probable?*	Severity of harm *Minimal, significant or severe*	Overall risk *Low, medium or high*	Compliance risk	Associated organisation risk
Inappropriate disclosure of personal CCTV data internally within your organisation due to a lack of appropriate controls being in place.	Unauthorised access to live and recorded CCTV footage	Remote	Significant	Low	Breach of data protection legislation	The ICO may require action, staff/system may need to be reviewed.
CCTV Cameras are sited in locations where people might reasonably expect privacy e.g. entrance to toilets.	Unanticipated recording of images by data subjects	Possible	Significant	Low	Breach of data protection legislation	

Step 5: Identify measures to reduce risk

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance, training & awareness or future security testing for systems). *Some example measures are listed at Annex C.*

Risk to individuals	**Measures to reduce or eliminate risk**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
Unauthorised access to live and recorded CCTV footage	Secure password protected server folders Limited access of staff users and managers as described in the CCTV Code of Practice document Log book kept of all access requests Internal requests are assessed on a case-by-case basis and documented using an internal request form	Reduced	Yes
Unanticipated recording of images by data subjects	Clear signage in place at ALL camera locations Privacy policies updated to include CCTV	Reduced	Yes

Appendix 1

	Step 6: Sign off and record the DPIA outcomes Who has approved the privacy risks involved in the project? What solutions need to be implemented? Further information: Read p. 30-31 of ICO Code of Practice

Risk	Approved solution	Approved by
Unauthorised access to live and recorded CCTV footage	Secure user and password protected storage on local server CCTV Code of Practice published	Gavin Green
Unanticipated recording of images by data subjects	Clear signage in ALL camera locations	Gavin green

Annex A – Special Category or ‘High Risk data’

Special category data is more sensitive, and so needs more protection. For example, information about an individual’s:

race; ethnic origin; politics; religion; trade union membership; genetics; biometrics (where used for ID purposes); health; sex life; or sexual orientation. (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/)

Annex B – Examples of individual, organisational and compliance risks

Example Risks To Individuals

- Inappropriate disclosure of personal data internally within your organisation due to a lack of appropriate controls being in place.
- Accidental loss of electronic equipment by organisation's personnel may lead to risk of disclosure of personal information to third parties.
- Breach of data held electronically by "hackers".
- Vulnerable individuals or individuals about whom sensitive data is kept might be affected to a very high degree by inappropriate disclosure of personal data.
- Information released in anonymised form might lead to disclosure of personal data if anonymisation techniques chosen are not to be effective.
- Personal data being used in a manner not anticipated by data subjects due to an evolution in the nature of the project.
- Personal data being used for purposes not expected by data subjects due to failure to explain effectively how their data would be used.
- Personal data being used for automated decision making may be seen as excessively intrusive.
- Merging of datasets may result in a data controller having far more information about individuals than anticipated by the individuals.
- Merging of datasets may inadvertently allow individuals to be identified from anonymised data.
- Use of technology capable of making visual or audio recordings may be unacceptably intrusive.
- Collection of data containing identifiers may prevent users from using a service anonymously.
- Data may be kept longer than required in the absence of appropriate policies.
- Data unnecessary for the project may be collected if appropriate policies not in place, leading to unnecessary risks.
- Data may be transferred to countries with inadequate data protection regimes.

Organisational Risks

- Failure to comply with the GDPR may result in investigation, administrative fines, prosecution, or other sanctions. Failure to adequately conduct a DPIA where appropriate can itself be a breach of the GDPR.
- Data breaches or failure to live up to staff/parent/student expectations regarding privacy and personal data are likely to cause reputational risk.
- Public distrust of your organisation's use of personal information may lead to a reluctance on the part of individuals to deal with your organisation.
- Problems with project design identified late in the design process, or after completion, may be expensive and cumbersome to fix.
- Failure to manage how your organisation keeps and uses information can lead to inefficient duplication, or the expensive collection and storage of unnecessary information. Unnecessary processing and retention of information can also leave you at risk of non-compliance with the GDPR.
- Any harm caused to individuals by reason of mishandling of personal data may lead to claims for compensation against your organisation. Under the GDPR you may also be liable for non-material damage.

Compliance Risks

- Your organisation may face risks of prosecution, significant financial penalties, or reputational damage if you fail to comply with the GDPR. Individuals affected by a breach of the GDPR can seek compensation for both material and non-material damage.
- Failure to carry out a DPIA where appropriate is itself a breach of the legislation, as well as a lost opportunity to identify and mitigate against the future compliance risks a new project may bring.

Annex C – Example measures to reduce risk

Every project will have its own unique circumstances and risk profile, so there is no “one size fits all” set of data privacy solutions which may be adopted. However, the following are examples of data protection measures, some of which may be applied in a range of different scenarios:

- Deciding not to collect or store particular types of information.
- Putting in place strict retention periods, designed to minimise the length of time that personal data is retained.
- Reviewing physical and/or IT security in your organisation or for a particular project team and making appropriate improvements where necessary.
- Conducting general or project-specific training to ensure that personal data is handled securely.
- Creating protocols for information handling within the project, and ensuring that all relevant staff are trained in operating under the protocol.
- Producing guidance for staff as reference point in the event of any uncertainty relating to the handling of information.
- Assessing the need for new IT systems to safely process and store the data, and providing staff with training in any new system adopted.
- Assessing the portability of using anonymised or pseudonymised data as part of the project to reduce identification risks, and developing an appropriate anonymisation protocol if the use of anonymised data is suitable.
- Ensuring that individuals are fully informed about how their information will be used.
- Providing a contact point for individuals to raise any concerns they may have with your organisation.
- If you are using external data processors, selecting appropriately experienced data processors and putting in place legal arrangements to ensure compliance with data protection legislation.
- Deciding not to proceed with a particular element of a project if the data privacy risks associated with it are inescapable and the benefits expected from this part of the project cannot justify those risks.

In most cases, there are some data protection risks which cannot be eliminated or reduced. These risks can be accepted if they are proportionate to the outcomes that will be achieved by proceeding with the project notwithstanding the risk. Any decisions to accept data protection risks should be recorded in the data protection risk register, or otherwise in accordance with your project management process.

At this stage, you should also ensure that the project will be in compliance with data protection laws. In particular, you should consider whether the project complies with the data protection principles, and ensuring that you have a good legal basis for processing personal data.

Appendix 2 – Google Form exemplar:

Google form link for request of CCTV footage access is here:
https://docs.google.com/forms/d/e/1FAIpQLScIOa3ZpqSoSlpLYv_QZRFzOfDqtIl3ASZ2T0eFgfeHSPuMLw/viewform

CCTV request for Footage Access

Please fill out all relevant details in this form to request access to CCTV footage as required.
NOTE footage will only be accessed if it is considered appropriate by the CCTV data manager. Data is only stored for 14 days; outside of this time we will not be able to recover footage.
Once you have filled in this form it will be sent to the Data Manager for approval; the more information you can supply in this form the quicker access will be given and footage retrieved.

This form is automatically collecting email addresses for Fakenham Academy users. Change settings

Name of Person making Request *

Short answer text

Date of Request *

Month, day, year

Time and Length of Footage Requested *

Short answer text

Location of CCTV camera/incident where footage is be recovered *

- [ ] Main Entrance
- [ ] Facing NES House
- [ ] T1 IT Suite
- [ ] Front of Tech Block
- [ ] Withdrawal booths 1-3
- [ ] Withdrawal Booth's 4-6
- [ ] Withdrawal L-shape Room
- [ ] Withdrawal Back Room
- [ ] KS3 Confab
- [ ] Outside Assistant Principal Office
- [ ] KS4 Confab
- [ ] Dining Room Servery
- [ ] Perowne Boys Toilets
- [ ] Perowne Eating Area Art end
- [ ] Perowne eating Area Science End
- [ ] Perowne Facing Field
- [ ] Reception
- [ ] Lancastrian Block front

Nature of incident requested *

Choose

Nature of Footage Required *

Choose

Explain why Footage is required *

Your answer

Explain how the Footage will be used *

Your answer

SUBMIT

Never submit passwords through Google Forms.

The form writes back requested data to a secure Google spreadsheet which is accessible only by the managers and support staff listed in this document.
This creates a workflow of authorisation that generates a Google document file that is archived with the given information.

Appendix 3

The Request for CCTV footage form generates a spreadsheet which then generates a full document of the data request which is time and date stamped and digitally signed off by CCTV manager for full authorisation.
This document is archived in a secure Google folder which is accessible only by named staff members as listed in this CCTV policy.

Exemplars of on site signage:

Exterior Signage:

Interior Signage (note that sound will not be enabled on most cameras)

Appendix 4: Proposals for New Camera Locations:

Below section for proposals of new camera locations pending authorisation from SLT/ Governors. (cameras authorised and installed highlighted in RED)

1.