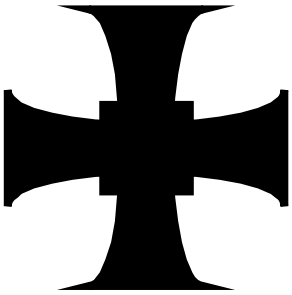
TRINITY SCHOOL



A CHURCH OF ENGLAND ACADEMY

DATA PROTECTION POLICY

Full Governing Body
Review: November 2015
Ratified by the full Governing Body: January 2016
Next review: November 2017

1. Aim

The aim of this policy is to ensure that Trinity School acts in ways which are consistent with the UK Data Protection Act (1998) – Code of Practice on Data Protection for Schools.

Trinity School is committed to protecting the rights and privacy of individuals – students and staff and others, in accordance with the Data Protection Act.

2. Purposes

Like all schools, Trinity School needs to have and to use certain information about its staff, students and other individuals with whom it has a relationship for various purposes. These include:

- the recruitment and payment of staff, and matters relating to their employment;
- the administration of the school's curriculum, and timetable;
- the monitoring and reporting of students' progress, including attendance and other pastoral information which allows us to enact our duty of care for students;
- monitoring behaviour and rewarding students;
- organising education visits, including residentials;
- collecting fees for examinations and trips etc. ;
- fulfilling our legal obligations to funding bodies and to government departments, to other agencies outside the school.

There may be other purposes beyond this list for which the school will have the need to have and to use information about students and staff and other individuals.

Trinity School will seek to ensure that all this information about individuals is collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully. We will seek to comply with various legal obligations, including the obligations imposed on it by the Data Protection Act, 1998.

3. Associated School Policies

- Overarching Safeguarding Statement
- Child Protection Policy
- E-Safety Policy and Acceptable Use Agreements
- CCTV Procedures (see Appendix D)
- Health and Safety Policy
- Procedures for Using Pupils' Images
- Whole School Behaviour Policy

4. Compliance

This policy applies to all staff and students of Trinity School. Any breach of this policy, or of the Act itself, will be considered an offence and the school's disciplinary procedures could be invoked.

We expect other agencies who work with us to have their own Data Protection policy and to work with us on the basis of compliance with the Act, with their own policy and with ours. The various departments in the school who are responsible for dealing with external agencies will take responsibility for ensuring that such agencies work with us in this way to protect individuals' data.

The Information Commissioner's Office (ICO) https://ico.org.uk/ gives further detailed guidance and Trinity School undertakes to adopt and comply with ICO guidance.

5. The Data Protection Act, 1998

The Act came into force on 1 March 2000. It regulates the use and storage of personal data, and protects the rights and privacy of all living individuals (including children). It gives all individuals, who are the subject of personal data, a general right of access to their personal data. Individuals can exercise the right to gain access to their information by means of a 'subject access request'. Personal data is information relating to an individual and may be in hard or soft copy (paper/ manual files; electronic records; photographs; CCTV images), and may include facts or opinions about a person.

The DPA also sets out specific rights for school students in relation to educational records held within the state education system. These rights are set out in separate education regulations 'The Education (Student Information) (England) Regulations 2000'. For more detailed information on these Regulations see the Data Protection Code of Practice for Schools (CoP) on the ICO website.

6. Responsibilities under the DPA

Trinity School will be the 'data controller' under the terms of the legislation – this means it is ultimately responsible for controlling the use and processing of the personal data.

The Co-Headteachers of this school are responsible for all day-to-day data protection matters, and will be responsible for ensuring that all members of staff and relevant individuals abide by this policy, and for developing and encouraging good information handling within the school.

The Co-Headteachers are also responsible for ensuring that the school's notification is kept accurate. Details of the school's notification can be found on the Office of the Information Commissioner's website https://ico.org.uk/.

Compliance with the legislation is the responsibility of all members of the school who process personal information. Individuals who provide personal data to the school are responsible for ensuring that the information is accurate and up-to-date.

Definitions

Data Controller:	Any individual or organisation who controls personal data, in this instance the School.
Personal Data:	Data which relates to a living individual who can be identified. Addresses and telephone numbers are particularly vulnerable to abuse, but so can names and photographs be, if published in the press, Internet or media.
Sensitive Personal Data:	Personal data relating to an individual's race or ethnic origin, political opinions, religious beliefs, physical/mental health, trade union membership, sexual life and criminal activities.
Relevant Filing System:	Also known as manual records i.e. a set of records which are organised by reference to the individual/their criteria and are structured in such a way as to make specific information readily accessible e.g. personnel records, microfiches.
Data Subject:	An individual who is the subject of the personal data, for example, employees, pupils, claimants etc.
Processing:	Obtaining, recording or holding data or carrying out any operation on the data including organising, adapting, altering, retrieving, consulting, using, disclosing, disseminating, aligning, blocking, erasing or destroying the data.
Accessible Records:	Any records which are kept by the Organisation as part of a statutory duty, e.g. pupil records, housing tenancy records, social services records.
Parent:	Has the meaning given in the Education act 1996, and includes any person having parental responsibility or care of a child.

7. Data Protection Principles

The legislation places a responsibility on every company which uses and stores information about people to deal with all personal data in keeping with the eight principles. In order to comply with its obligations, Trinity School undertakes to:

1. *Process personal data fairly and lawfully and communicate with individuals*

Trinity School will take all reasonable efforts to ensure that individuals whose information we have (data subjects) are informed of the identity of the data controller; the purposes of the processing; any disclosures to third parties that are envisaged; given an indication of the period for which the data will be kept, and any other information which may be relevant.

2. *Process the data for the specific and lawful purpose for which it collected that data, and not further process the data in a manner incompatible with this purpose.*

Trinity School will ensure that the reason for which it collected the data originally is the only reason for which it processes those data, unless the individual is informed of any additional processing before it takes place.

3. *Ensure that the data is adequate, relevant and not excessive in relation to the purpose for which it is processed.*

Trinity School will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this in mind. If any irrelevant data are given by individuals, they will be destroyed immediately.

4. *Keep personal data accurate and, where necessary, up to date*

Trinity School will review and update all data on a regular basis.

It is the responsibility of the individuals giving their personal data to ensure that this is accurate, and each individual should notify the school if, for example, a change in circumstances mean that the data needs to be updated. It is the responsibility of the school to ensure that any notification regarding the change is noted and acted upon.

5. *Only keep personal data for as long as is necessary*

Trinity School undertakes not to retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements. This means that Trinity School will undertake a regular review of the information held and implement a weeding process when, for example, students or a member of staff leave the school.

Trinity School will dispose of any personal data in a way that protects the rights and privacy of the individual concerned.

6. *Process personal data in accordance with the rights of the data subject under the legislation*

Individuals have various rights under the legislation including:

- a right to be told the nature of the information the school holds and any parties to whom this may be disclosed
- a right to prevent processing likely to cause damage or distress
- a right to prevent processing for purposes of direct marketing
- a right to be informed about the mechanics of any automated decision taking process that will significantly affect them
- a right not to have significant decisions that will affect them taken solely by automated process
- a right to sue for compensation if they suffer damage by any contravention of the legislation
- a right to take action to rectify, block, erase, or destroy inaccurate data

- a right to request that the Office of the Information Commissioner assess whether any provision of the Act has been contravened

Trinity School will only process personal data in accordance with individuals' rights.

7. *Put appropriate technical and organisational measures in place against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of data*

All members of staff are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third parties. Trinity School will ensure that all personal data is accessible only to those who have a valid reason for using it.

Trinity School will have in place appropriate security measures e.g. ensuring that hard copy personal data is kept in lockable filing cabinets/ cupboards with controlled access; keeping all personal data in a lockable room with key-controlled access; password protecting personal data held electronically; archiving personal data on disks which are then kept securely (lockable cabinet; placing any PCs or terminals, CCTV camera screens etc. that show personal data so that they are not be visible except to authorised staff.

In addition, Trinity School will put in place appropriate measures for the deletion of personal data – manual records will be shredded or disposed of as 'confidential waste', and appropriate contract terms will be put in place with any third parties undertaking this work. Hard drives of redundant PCs will be wiped clean before disposal, or if that is not possible, destroyed physically.

This policy also applies to staff and students who process personal data 'off-site', e.g., when working at home, and in such circumstances additional care must be taken regarding the security of the data.

8. *Ensure that no personal data are transferred to a country or a territory outside the European Economic Area unless that country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data*

Trinity School will not transfer data to such territories without the explicit consent of the individual. This also applies to publishing information on the Internet – because transfer of data can include placing data on a website that can be accessed from outside the EEA – so Trinity School will always seek the consent of individuals before placing any personal data (including photographs) on its website. There will be a general consent for this at the start of a student's time in the school.

If the school collects personal data in any form via its website, it will provide a clear and detailed privacy statement prominently on the website, and wherever else personal data is collected.

8. Consent as a Basis for Processing

Although it is not always necessary to gain consent from individuals before processing their data, it is often the best way to ensure that data is collected and processed in an open and transparent manner. Consent is especially important when schools are processing any sensitive data, as defined by the legislation.

Trinity School understands consent to mean that the individual has been fully informed of the intended processing and has signified their agreement (e.g. via signing a form), whilst being of a sound mind and without having any undue influence exerted upon them. Consent obtained on the basis of misleading information will not be a valid basis for processing. Consent cannot be inferred from the non-response to a communication.

Trinity School will ensure that any forms used to gather data on an individual will contain a statement (fair collection statement) explaining the use of that data, how the data may be disclosed, and also indicate whether or not the individual needs to consent to the processing.

Trinity School will ensure that if the individual does not give her consent for the processing, and there is no other lawful basis on which to process the data, then steps will be taken to ensure that processing of that data does not take place.

9. Fair Processing

Under the "Fair Processing" requirements in the Data Protection Act, the school will inform staff and separately parents/carers of all pupils/students of the data they hold on the staff member or pupils/students, the purposes for which the data is held and the third parties (e.g. LA, DfE, QCA, Connexions etc.) to whom it may be passed. This fair processing notice, now known as a Privacy Notice will be passed to staff when they join the school and to parents/carers via a specific letter home. Parents/carers of young people who are new to the school will also be provided with the Privacy Notice in the form of a letter home.

A copy of Trinity School's Privacy Notices can be found in Appendices B and C.

10. Subject Access Rights

Individuals have a right to have access to any personal data relating to them which are held by the school. Any individual wishing to exercise this right should apply in writing to the Co-Headteachers. Any member of staff receiving such a request should forward this to the Co-Headteachers.

The school reserves the right to charge a fee for data subject access requests.

Under the terms of the legislation, any such requests must be complied with within 40 days.

Note: In the case of any written request from a parent regarding their own child's record, access to the record will be provided within 15 school days in accordance with the current Education (Pupil Information) Regulations.

11. Disclosure of Data

Only disclosures which have been notified under the school's DP notification must be made and therefore staff and students should exercise great caution when asked to disclose personal data held on another individual or third party. Advice should be sought from a member of the Senior Leadership Team or the ICT Network Manager and team.

Trinity School undertakes not to disclose personal data to unauthorised third parties, including family members, friends, government bodies, and in some circumstances, the police.

Legitimate disclosures may occur in the following instances:

- the individual has given their consent to the disclosure
- the disclosure has been notified to the ICO and is in the legitimate interests of the school
- the school is legally obliged to disclose the information
- the disclosure is required for the performance of a contract
- the disclosure is necessary for safeguarding or criminal investigation purposes.

The School will, in general, only disclose data about individuals with their consent. However there are circumstances under which the School's authorised officer may need to disclose data without explicit consent for that occasion.

These circumstances are strictly limited to:

- Pupil data disclosed to authorised recipients related to education and administration necessary for the school to perform its statutory duties and obligations.
- Pupil data disclosed to authorised recipients in respect of their child's health, safety and welfare.
- Pupil data disclosed to parents in respect of their child's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of the school.

- Staff data disclosed to relevant authorities e.g. in respect of payroll and administrative matters.
- Unavoidable disclosures, for example to an engineer during maintenance of the computer system. In such circumstances the engineer would be required to sign a form promising not to disclose the data outside the school. Officers and IT personnel writing on behalf of the LA are IT liaison/data processing officers, for example in the LA, are contractually bound not to disclose personal data.
- Only authorised and trained staff are allowed to make external disclosures of personal data. Data used within the school by administrative staff, teachers and welfare officers will only be made available where the person requesting the information is a professional legitimately working within the school who **need to know** the information in order to do their work. The school will not disclose anything on pupils' records which would be likely to cause serious harm to their physical or mental health or that of anyone else – including anything where suggests that they are, or have been, either the subject of or at risk of child abuse.

In no circumstances will Trinity School sell any of its databases to a third party.

12. Publication of school information
Trinity School publishes various items which will include some personal data, for example:

- our internal telephone directory
- event information
- staff information
- lists of students

It may be that in some circumstances an individual wishes their data processed for such reasons to be kept confidential, or restricted to internal school access only.
Therefore it is Trinity School's policy to offer an opportunity to opt-out of the publication of such when collecting the information.

Staff records will remain of a confidential nature between the Co-Headteachers and that member of staff and, where appropriate, the school HR manager.

13. Email
It is the policy of Trinity School to ensure that senders and recipients of email are made aware that under the DPA, and Freedom of Information legislation, the contents of email may have to be disclosed in response to a request for information. One means by which this will be communicated will be by a disclaimer on the school's email.

Under the Regulation of Investigatory Powers Act 2000, Lawful Business Practice Regulations, any email sent to or from the school may be accessed by someone other than the recipient for system management and security purposes.

14. CCTV
There is a CCTV system operating within Trinity School for the purpose of protecting school members and property. Trinity School will only process any personal data obtained by the CCTV system in a manner which ensures compliance with the legislation.

For detailed guidance on CCTV refer to the ICO 'In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Data', October 2014 which can be found at https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf and the school CCTV Procedures appended to this Policy.

15. Data and Computer Security
Trinity School undertakes to ensure security of personal data by the following general methods (precise details cannot, of course, be revealed):

Physical Security
Appropriate building security measures are in place, such as alarms, window bars, deadlocks and computer hardware cable locks. Only authorised persons are allowed in computer rooms. Disks, tapes and printouts are locked away securely when not in use. Visitors to the school are required to sign in and out, to wear identification badges whilst in the school and are, where appropriate, accompanied.

Logical Security

- Security software is installed on all computers containing personal data.
- The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them.
- A safe and secure username/password system which gives students fixed passwords is managed by the ICT Services Manager. User names and passwords must never be shared.
- Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.
- All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.
- Personal data can only be stored on school equipment (this includes computers and portable storage media). Private equipment (i.e. owned by the users) must not be used.
- When personal data is stored on any portable computer system, USB stick or any other removable media:

    - the data must be encrypted and password protected;
    - the device must be password protected (many memory sticks/cards and other mobile devices cannot be password protected);
    - the device must offer approved virus and malware checking software;
    - the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

- The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.

Procedural Security
In order to be given authorised access to the computer, staff will have to undergo checks and will sign a confidentiality agreement. All staff are trained in their Data Protection obligations and their knowledge updated as necessary. Computer printouts as well as source documents are shredded before disposal. Further information can be found in the school e-Safety Policy.

Overall security policy for data is determined by the Co-Headteachers and is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent. The School's security policy is kept in a safe place at all times.

Any queries or concerns about security of data in the school should in the first instance be referred to the Co-Headteachers.

Individual members of staff can be personally liable in law under the terms of the Data Protection Acts. They may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of this Data Protection Policy will be treated as disciplinary matter, and serious breaches could lead to dismissal.

16. Secure transfer of data and access out of school
The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location.
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school.
- When data is required by an authorised user from outside the school premises (for example, by a teacher or student working from their home or a contractor) they must have secure remote access to the management information system (MIS) or learning platform.
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority in this event. (NB. to carry encrypted material is illegal in some countries.)

17. Disposal of Data
The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of protected data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten and other media must be shredded, incinerated or otherwise disintegrated for data.

A Destruction Log will be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

18. Training & Awareness
All staff will receive data handling awareness/data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff;
- Staff meetings/briefings/Inset;
- Day to day support and guidance from Responsible Persons.

19. Enquiries
Information about the school's Data Protection Policy is available from the Co-Headteachers. General information about the Data Protection Act can be obtained from the Information Commissioners Office https://ico.org.uk/.

A copy of this policy will be available to all employees and covered in new staff Induction Training. It will be reviewed biennially, added to, or modified from time to time and may be supplemented in appropriate cases by further statements and procedures relating to the work of the particular groups of workers.

ACCESS TO PERSONAL DATA REQUEST

(Subject Access Request – SARS)

DATA PROTECTION ACT 1998 (Section 7)

Enquirer's Surname		**Enquirer's Forenames**	
Enquirer's Address			
Enquirer's Postcode:			
Enquirer's Tel No.			
Are you the person who is the subject of the records you are enquiring about (i.e. the "Data Subject")?			**YES / NO**
If NO,			
Do you have parental responsibility for a child who is the "Data Subject" of the records you are enquiring about?			**YES / NO**
If YES,			
Name of child or children about whose personal data records you are enquiring:	_____ _____ _____ _____		
Description of Concern / Area of Concern			
Description of Information or Topic(s) Requested (In your own words)			
Additional Information			

Please despatch Reply to: *(if different from enquirer's details as stated on this form)*

Name

Address

Postcode

DATA SUBJECT DECLARATION

I request that the School search its records based on the information supplied above under Section 7 (1) of the Data Protection Act 1998 and provide a description of the personal data found from the information described in the details outlined above relating to me (or my child/children) being processed by the School.

I agree that the reply period will commence when I have supplied sufficient information to enable the School to perform the search.

I consent to the reply being disclosed and sent to me at my stated address (or to the Despatch Name and Address above who I have authorised to receive such information).

Signature of "Data Subject" (or Subject's Parent) _____

Name of "Data Subject" (or Subject's Parent) (PRINTED) _____

Dated _____

Trinity School PRIVACY NOTICE for the school workforce employed or otherwise engaged to work at a school

Privacy Notice - Data Protection Act 1998

We, Trinity School are the Data Controller for the purposes of the Data Protection Act. Personal data is held by the school about those employed or otherwise engaged to work at the school. This is to assist in the smooth running of the school and/or enable individuals to be paid. This personal data includes some or all of the following: identifiers such as name and National Insurance Number; characteristics such as ethnic group; employment contract and remuneration details; post "A" level qualifications; and absence information.

The collection of this information will benefit both national and local users by:

- improving the management of school workforce data across the sector;
- enabling a comprehensive picture of the workforce and how it is deployed to be built up;
- informing the development of recruitment and retention policies;
- allowing better financial modelling and planning;
- enabling ethnicity and disability monitoring; and
- supporting the work of the School Teachers' Review Body.

We are required by law to pass on some of this data to:

- the Local Authority (LA)
- the Department for Education (DfE)

If you require more information about how the Local Authority (LA) and/or DfE store and use this data please go to the following websites:
http://www.cumbria.gov.uk/childrensservices/schoolsandlearning/schools/privacynotice.asp and

http://media.education.gov.uk/assets/files/doc/w/what%20the%20department%20does%20with%20data%20on%20pupils%20and%20children.doc

If you are unable to access these websites we can send you a copy of this information. Please contact the LA or DfE as follows:

- Performance Unit, Children's Services
  The Lonsdale Building
  The Courts
  English Street — website: www.cumbria.gov.uk/childrensservices
  Carlisle — email: ros.dean@cumbria.gov.uk
  CA3 8NA — tel: 01228 221271
- Public Communications Unit
  Department for Education
  Sanctuary Buildings
  Great Smith Street
  London — email: http://www.education.gov.uk/help/contactus
  SW1P 3BT — Tel: 0370 000 2288
  website: https://www.gov.uk/government/organisations/department-for-education

We will not give information about you to anyone outside the school or LA without your consent unless the law and our rules allow us to.

Trinity School PRIVACY NOTICE for pupils

Dear Parent/Carer

The school is required to provide you with general information about the sort of data held electronically by us about pupils. Undernoted is a copy of a leaflet, produced by Cumbria Education Department detailing the types of information that various agencies involved in childcare hold about children. This information is required due to the 1998 Data Protection Act and is known as a 'Privacy Notice'. This replaces the 'Fair Processing Notice'.

Pupils and parents, as data subjects, have certain rights under the Data Protection Act 1988, including a general right to be given access to personal data held about them by any data controller. There is a presumption (endorsed by legal guidance issued by the Information Commissioner) that children of twelve years of age and over have sufficient maturity to exercise their rights themselves, though in practice there will be exceptions to this.

As a school we are issuing a Privacy Notice to all parents of students in Years 7-11 and all students over the age of 16. However we would ask that if your child is over the age of 12 that you share this information with them.

Privacy Notice - Data Protection Act 1998

We at Trinity School are a data controller for the purposes of the Data Protection Act. We collect information from you and may receive information about your child from their previous school and the Learning Records Service. We hold this personal data and use it to:

- Support their teaching and learning
- Monitor and report on their progress
- Provide appropriate pastoral care
- Assess how well their school is doing

This information includes contact details, national curriculum assessment results, attendance information[1] and personal characteristics such as ethnic group, any special educational needs and relevant medical information. *If they are enrolling for post 14 qualifications we will be provided with their unique learner number (ULN) by the Learning Records Service and may also obtain from them details of any learning or qualifications they have undertaken.*

We will not give information about your child to anyone outside the school without your consent unless the law and our rules allow us to.

We are required by law to pass some information about your child to the Department for Education (DfE) and, in turn, this will be available for the use(s) of the Local Authority.

If you want to see a copy of the information about your child that we hold and/or share, please contact Mrs Jacklyn Hunton at the school.

If you require more information about how the Local Authority (LA) and/or DfE store and use your child's information, then please go to the following websites:

http://www.cumbria.gov.uk/childrensservices/schoolsandlearning/schools/privacynotice.asp

http://www.education.gov.uk/researchandstatistics/childrenandyoungpeople/a0064391/who-the-department-passes-pupil-data-to

If you are unable to access these websites we can send you a copy of this information. Please contact the LA or DfE as follows:

Performance Unit
Children's Services
The Lonsdale Building
The Courts
English Street
Carlisle
CA3 8NA

website: www.cumbria.gov.uk/childrensservices
email: ros.dean@cumbria.gov.uk
tel: 01228 221271

Public Communications Unit
Department for Education
Sanctuary Buildings
Great Smith Street
London
SW1P 3BT

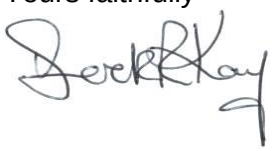
website: www.education.gov.uk
email: http://www.education.gov.uk/help/contactus
tel: 0370 000 2288

Inspira - Once your child is aged 13 or over, we are required by law to pass on certain information to the provider of youth support services in your area. Inspira is the local authority support service for young people aged 13 to 19 in England. We must provide the address of you and your child (and their date of birth) and any further information relevant to the support services' role.

However, until they are aged 16 or older, you can ask that no information beyond their name, address and date of birth (and your name and address) be passed on to the youth services provider. This right transfers to your child on their 16th birthday. Please inform Mrs J Hunton, at the school if this is what you wish.

For more information about young peoples' services, please go to the National Careers Service page at https://nationalcareerservice.direct.gov.uk/aboutus/Pages/default.aspx .

Yours faithfully



Derek Kay
Headteacher

REVIEW SHEET

The information in the table below details earlier versions of this document with a brief description of each review and how to distinguish amendments made since the previous version date (if any).

Version Number	Version Description	Date of Revision
2	Significant rewrite in line with the ICO 'In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Data' (May 2015)	September 2015

Contents

1 Introduction 17
1.1 Exemptions 17
2 Objectives of the CCTV Scheme 17
3 General Principles 18
4 Justification for Use of CCTV 19
4.1 Visual Recording 19
5 Operation of the System 20
6 Siting of Cameras 20
7 Covert Surveillance 21
8 Notification – Signage 21
9 Storage and Retention of Recorded Images 22
9.1 Storage 22
9.2 Retention 23
9.3 Access 23
10 Disclosure of Images 23
10.1 Requests by the Police 24
10.2 Subject Access Requests 24
10.3 Freedom of Information 25
11 Breaches of the Procedures (including security breaches) 25
12 Monitoring and Review 26
13 Complaints 27
14 Further Information 27

Appendix A - Annual Review of CCTV Systems (Checklist)

Appendix B - The Guiding Principles of the Surveillance Camera Code of Practice (ICO)

Appendix C - Requests by the Police Form

CCTV PROCEDURES

1. Introduction

The purpose of these Procedures is to regulate the use of CCTV and its associated technology in the monitoring of both the internal and external environs of the premises under the remit of Trinity School/Setting, hereinafter referred to as 'the school'.

The CCTV system is owned and operated by the school, the deployment of which is determined by the school senior leadership team.

These procedures follow the Information Commissioners Office 'In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Data' (May 2015); the Data Protection Act (DPA) guidelines and the School Data Protection Policy, both of which are held separately.

These Procedures will be subject to regular review to include consultation as appropriate with interested parties.

New CCTV systems will be introduced in consultation with staff, the school senior leadership team, students and parents/carers. Where systems are already in operation, their operation will be reviewed regularly in consultation with staff, the school senior leadership team, students and parents/carers.

1.1 Exemptions

The use of surveillance systems for limited household purposes is exempt from the DPA e.g. a video of a child in a nativity play recorded for the parent/carer's own family use is not covered by the DPA.

The covert surveillance activities of public authorities (refer to Section 7) are not covered here because they are governed by the Regulation of Investigatory Powers Act (RIPA) 2000. This type of recording is covert and directed at an individual or individuals.

The use of conventional cameras (not CCTV) by the news media or for artistic purposes, such as for film making, are not covered by these procedures as an exemption within the DPA applies to activities relating to journalistic, artistic and literary purposes.

2. Objectives of the CCTV Scheme

The system comprises a number of fixed and dome cameras located around the site both internally and externally for the purpose of enhancing security of the building and its associated equipment as well as creating a mindfulness among the occupants, at any one time, that a surveillance security system is in operation within and in the external environs of the premises during both the daytime and hours of darkness. CCTV surveillance at the school is intended for the purposes of:

- protecting the school buildings and assets, both during and after school hours;
- increasing the personal safety of staff, students and visitors;
- reducing the fear of crime;
- reducing the risk of bullying;
- reducing the incidence of crime and anti-social behaviour (including theft and vandalism);
- supporting the Police in a bid to deter and detect crime;
- assisting in identifying, apprehending and prosecuting offenders;
- protecting members of the public; and

- ensuring that the school rules are respected so that the school can be properly managed.

3. General Principles

The school as the corporate body has a statutory responsibility for the protection of its property, equipment and other plant as well providing a sense of security to its employees, students and invitees to its premises. The school owes a duty of care under the provisions of the Health and Safety at Work etc. Act, 1974 and associated legislation and utilises CCTV systems and their associated monitoring and recording equipment as an added mode of security and surveillance for the purpose of enhancing the quality of life of the school community by integrating the best practices governing the public and private surveillance of its premises. The use of CCTV, and the associated images and any sound recordings is covered by the Data Protection Act 1998. These Procedures outline the school's use of CCTV and how it complies with the Act. The school will treat the system and all information, documents and recordings obtained and used as data which are protected by the Act.

The school complies with the Information Commissioner's Office (ICO) CCTV Code of Practice to ensure it is used responsibly and safeguards both trust and confidence in its continued use. The ICO 'In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Data, May 2015 can be found at https://ico.org.uk/media/1542/cctv-code-of-practice.pdf

The Co-Headteachers are responsible for all day-to-day data protection matters, and they will be responsible for ensuring that all members of staff and relevant individuals abide by these procedures, and for developing and encouraging good information handling within the school. Trinity School is registered as a Data Controller on the Data Protection Register held by the Information Commissioner. Notification to the ICO is renewed annually.

All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images and sound. All operators are trained by the school data controller in their responsibilities under these CCTV Procedures. Staff using the surveillance system or information have been trained to ensure they comply with these procedures. In particular, they have been made aware of:

- What the school's arrangements are for recording and retaining information.
- How to handle the information securely.
- What to do if they receive a request for information, for example, from the police.
- How to recognise a subject access request and what to do if they receive one.

Monitoring for security purposes will be conducted in a professional, ethical and legal manner and any diversion of the use of CCTV security technologies and personnel for other purposes is prohibited e.g. monitoring of political or religious activities, or employee and/or student evaluations that would undermine the acceptability of the resources for use regarding critical safety and security objectives.

CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with all existing policies adopted by the school including the Data Protection Policy, Single Equality Scheme and Whole School Behaviour Policy (incorporating Anti-Bullying and Harassment strategies) etc.

Our procedures for video monitoring prohibits monitoring based on the characteristic and classification contained in Equality and other related legislation, for example race, gender, sexual orientation, national origin, disability etc. The system is in place to monitor suspicious behaviour and not individual characteristics.

Video monitoring of public areas for security purposes is limited to uses that do not violate the reasonable expectation of privacy as defined by Law.

Consideration will be given to both staff and students regarding possible invasions of privacy and confidentiality due to the location of a particular CCTV camera or associated equipment. The Head teacher will ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within the school and be mindful that no such infringement is likely to take place. The camera control will be monitored to ensure it is not in breach of the intrusion on intimate behaviour by persons in public changing and toilet areas.

Cameras will be used to monitor activities within the school and its car parks and other public areas to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and wellbeing of the school, together with its visitors.

Staff have been instructed that static cameras are not to focus on private homes, gardens and other areas of private property. Unless an immediate response to events is required, staff must not direct cameras at an individual, their property or a specific group of individuals, without an authorisation being obtained for Directed Surveillance to take place, as set out in the Regulation of Investigatory Power Act 2000 (RIPA).

The head teacher will approve any temporary cameras to be used during special events that have particular security requirements and ensure their withdrawal following such events. (Temporary cameras do not include mobile video equipment or hidden surveillance cameras used for criminal investigations).

When a zoom facility on a camera is being used, a second person will be present with the camera operator to guarantee that there is no unwarranted invasion of privacy.

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Data will only be released to the media for use in the investigation of a specific crime and with the written authority of the police. Data will never be released to the media for purposes of entertainment.

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

Warning signs, as required by the ICO Code of Practice have been placed at all access routes to areas covered by the school CCTV – refer to Section 8.

Information obtained through the CCTV system may only be released when authorised by the Co-Headteachers following consultation with the Chair of the Governing Body. Any requests for CCTV recordings/images from the Police will be fully recorded. If a law enforcement authority is seeking a recording for a specific investigation, any such request made should be made in writing.

4. Justification for Use of CCTV

4.1 Visual Recording

The Data Protection Act requires that data is "adequate, relevant and not excessive" for the purpose for which it is collected. This means that the school needs to be able to justify the obtaining and use of personal data by means of a CCTV system by conducting a Privacy Impact Assessment (PIA) – refer to the Information Commissioner's Office 'Conducting

Privacy Impact Assessments' Code of Practice https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf . We have considered the privacy issues involved with using surveillance systems and have concluded that their use is necessary and proportionate and address a pressing need that we have identified. We have considered less privacy intrusive methods of achieving this need where possible.

The use of CCTV to control the perimeter of the school buildings and entrances/exits for security purposes has been deemed to be justified by the Senior Leadership Team. The system is intended to capture images of intruders or of individuals damaging property or removing goods without authorisation for example.

In other areas of the school where CCTV has been installed, e.g. hallways, stairwells, locker areas, etc. the Co-Headteachers have demonstrated that there is a proven risk to security and/or health & safety and that the installation of CCTV is proportionate in addressing such issues that have arisen prior to the installation of the system.

CCTV systems will not be used to monitor normal teacher/student classroom activity in school.

5. Operation of the System

- The Scheme will be administered and managed by the Co-Headteachers, in accordance with the principles and objectives expressed within these procedures.
- The day-to-day management will be the responsibility of both the Senior Leadership Team and the IT Administrator or Facilities Manager
- The CCTV system will be operated 24 hours each day, every day of the year.

6. Siting of Cameras

The location of cameras is a key consideration. Use of CCTV to monitor areas where individuals would have a reasonable expectation of privacy would be difficult to justify. The school has endeavoured to select locations for the installation of CCTV cameras which are least intrusive to protect the privacy of individuals. Cameras placed so as to record external areas are positioned in such a way as to prevent or minimise recording of passers-by or of another person's private property.

CCTV video monitoring and recording of public areas in the school may include the following:

- **Protection of school buildings and property:** The building's perimeter, entrances and exits, lobbies and corridors, special storage areas, cashier locations, receiving areas for goods/services.
- **Monitoring of Access Control Systems:** Monitor and record restricted access areas at entrances to buildings and other areas.
- **Verification of Security Alarms:** Intrusion alarms, exit door controls, external alarms.
- **Video Patrol of Public Areas:** Parking areas, main entrance/exit gates, Traffic Control.
- **Criminal Investigations (carried out by the Police):** Robbery, burglary and theft surveillance.

The following points were considered when the CCTV cameras were installed:

- Camera locations were chosen carefully to minimise viewing spaces that are not of relevance to the purposes for which we are using CCTV.

- Where CCTV has been installed to deal with a specific problem, we have considered setting the system up so it only records during the time when the problem usually occurs.
- The cameras have been sited to ensure that they can produce images of the right quality, taking into account their technical capabilities and the environment in which they are placed.
- Cameras are suitable for the location, bearing in mind the light levels and the size of the area to be viewed by each camera.
- We have checked that a fixed camera positioned in winter will not be obscured by the growth of plants and trees in the spring and summer.
- Cameras are sited so that they are secure and protected from vandalism.
- The system will produce images of sufficient size, resolution and frames per second.

7. Covert Surveillance

The school will not engage in covert surveillance.

Certain law enforcement agencies may request to carry out covert surveillance on school premises. Such covert surveillance may require a Court Order. Accordingly, any such request made by law enforcement agencies will be requested in writing. The covert surveillance activities of public authorities are not covered here because they are governed by the Regulation of Investigatory Powers Act (RIPA) 2000. This type of recording is covert and directed at an individual or individuals.

8. Notification – Signage

The Co-Headteachers will provide a copy of these CCTV Procedures on request to staff, students, parents/carers and visitors to the school. These Procedures describe the purpose and location of CCTV monitoring, a contact number for those wishing to discuss CCTV monitoring and guidelines for its use.

We must let people know when they are in an area where a surveillance system is in operation. The most effective way of doing this is by using prominently placed signs at the entrance to the surveillance system's zone and reinforcing this with further signs inside the area. Clear and prominent signs are particularly important where the surveillance systems are very discreet, or in locations where people might not expect to be under surveillance. As a general rule, signs should be more prominent and frequent in areas where people are less likely to expect that they will be monitored by a surveillance system.

Signs should:

- be clearly visible and readable;
- contain details of the organisation operating the system, the purpose for using the surveillance system and who to contact about the scheme (where these things are not obvious to those being monitored);
- include basic contact details such as a simple website address, telephone number or email contact; and be an appropriate size.

Adequate signage will be placed at each location in which a CCTV camera(s) is sited to indicate that CCTV is in operation. Adequate signage will also be prominently displayed at the entrance to the school property. Signage shall include the name and contact details of the data controller as well as the specific purpose(s) for which the CCTV camera is in place in each location.

Trinity School

All staff will be made aware of what to do or who to contact if a member of the public makes an enquiry about the surveillance system.

In exceptional circumstances where audio recording is being used, this should be stated explicitly and prominently. It should also be clearly stated if audio recording is used for a different or further purpose than visual recording.

9. Storage and Retention of Recorded Images

9.1 Storage

Recorded material will be stored in a way that maintains the integrity of the information – recorded material is stored on computer hard disc. This is to ensure that the rights of individuals recorded by surveillance systems are protected and that the information can be used effectively for its intended purpose. Recorded material is stored in a secure environment – school server room with a log of access kept by ICT Services Manager. Access to recorded material is restricted to Head teacher ICT Services Manager and Facilities Manager. All recorded information is secure.

Supervising the access and maintenance of the CCTV System is the responsibility of the Co-Headteachers. The Co-Headteachers may delegate the administration of the CCTV System to the ICT Services Manager. In certain circumstances, the recordings may also be viewed by other individuals in order to achieve the objectives set out above e.g. the Police, the Deputy Head teacher, Facilities Manager, the relevant Year Head, other members of the teaching staff, representatives of the DfE, representatives of the HSE and/or the parent

of a recorded student. When CCTV recordings are being viewed, access will be limited to authorised individuals on a need-to-know basis.

We will keep a record or audit trail showing how the information must be handled if it is likely to be used as evidence in court. Once there is no reason to retain the recorded information, it will be deleted. Exactly when we decide to do this will depend on the purpose for using the surveillance systems. A record or audit trail of this process will also be captured.

CCTV images are digitally recorded. It is important that our information can be used by appropriate law enforcement agencies if it's required.

- Copying of CCTV footage does not interfere with live recordings
- System will record direct to DVD
- Image is watermarked to guarantee authenticity
- DVD recording had built in media player
- DVD's sent to external agencies will be logged by the operator

9.2 Retention

The Data Protection Acts states that data "shall not be kept for longer than is necessary for" the purposes for which it was obtained. As a data controller, Trinity School needs to be able to justify this retention period. For a normal CCTV security system, it would be difficult to justify retention beyond a month (28 days), except where the images identify an issue – such as a break-in or theft and those particular images/recordings are retained specifically in the context of an investigation/ prosecution of that issue.

Accordingly, the images captured by the CCTV system will be retained for a maximum of 30 days, except where the image identifies an issue and is retained specifically in the context of an investigation/prosecution of that issue.

- The School will retain CCTV images for a maximum of 30 days
- The system will overwrite data as new images are recorded
- Data taken off onto DVD will be kept in a secure location – ICT Office Safe
- Data recorded onto DVD will be logged by the Operator

9.3 Access

Digitally captured images and the monitoring equipment will be securely stored in a restricted area. Unauthorised access to that area will not be permitted at any time. The area will be locked when not occupied by authorised personnel.

Access to the CCTV system and stored images will be restricted to authorised personnel only i.e. the Co-Headteachers, ICT Services Manager.

10. Disclosure of Images

There will be no disclosure of recorded data to third parties other than to authorised personnel such as the Police and service providers to the school where these would reasonably need access to the data (e.g. investigators). In relevant circumstances, CCTV footage may be disclosed:

- To the Police where the school is required by law to make a report regarding the commission of a suspected crime; or

- Following a request by the Police when a crime or suspected crime has taken place and/or when it is suspected that illegal/anti-social behaviour is taking place on the school property, or
- To the HSE and/or any other statutory body charged with child safeguarding; or
- To assist the Co-Headteachers in establishing facts in cases of unacceptable student behaviour, in which case, the parents/carers will be informed. The data may be used within the school's discipline and grievance procedures as required, and will be subject to the usual confidentiality requirements of those procedures; or
- To data subjects (or their legal representatives), pursuant to an access request where the time, date and location of the recordings is furnished to the school; or
- To individuals (or their legal representatives) subject to a court order; or
- To the school's insurance company where the insurance company requires same in order to pursue a claim for damage done to the insured property.

Only authorised and trained staff are allowed to make external disclosures of CCTV footage Head teacher, ICT Services Manager, Facilities Manager

Data will never be placed in the internet and will not be released to the media. Information may be released to the media for identification purposes but this must NOT be done by anyone other than a law enforcement agency.

Once we have disclosed information to another body, such as the police, they become the Data Controller for the copy they hold. It is their responsibility to comply with the DPA in relation to any further disclosures.

10.1 Requests by the Police

Information obtained through video monitoring will only be released when authorised by the Co-Headteachers.

10.2 Subject Access Requests

Staff involved in operating the surveillance system have been trained to recognise a subject access request. A log of the requests received will be kept and how they were dealt with.

On written request, any person whose image has been recorded has a right to be given a copy of the information recorded which relates to them, provided always that such an image/recording exists i.e. has not been deleted and provided also that an exemption/prohibition does not apply to the release. Where the image/recording identifies another individual, those images may only be released where they can be redacted/anonymised so that the other person is not identified or identifiable. Where a subject access request is received for surveillance footage or other information, we are required to provide the data subject with a copy of all the information caught by the request that constitutes their personal data, unless an exemption applies. This must be done by supplying them with a copy of the information in a permanent form. There are limited circumstances where this obligation does not apply.

The first is where the data subject agrees to receive their information in another way, such as by viewing the footage. The second is where the supply of a copy in a permanent form is not possible or would involve disproportionate effort. The ICO's subject access code of practice makes clear this provision is only likely to be relevant in exceptional cases. If the data subject refuses an offer to view the footage or the data subject insists on a copy of the footage, then we must consider ways in which we can provide the data subject with this information.

We will always first attempt to provide the footage to the individual, or invite the data subject to a viewing if they consent to this.

If an individual agrees to a viewing of the footage but subsequently asks for that footage, it may be necessary, or at least good practice, to provide this footage where possible.

To exercise their right of access, a data subject must make an application in writing to the Co-Headteachers. The school may charge up to £10 for responding to such a request and must respond to requests **within 40 calendar days** of receiving the written request and fee.

Requests for Data Subject Access should be made on an application form available from the Head teacher (refer to the school Data Protection Policy for further details).

A person should provide all the necessary information to assist the school in locating the CCTV recorded data, such as the date, time and location of the recording. If the image is of such poor quality as not to clearly identify an individual, that image may not be considered to be personal data and may not be handed over by the school. The school reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an on-going investigation.

In giving a person a copy of their data, the school may provide a still/series of still pictures, a tape or a disk with relevant images. However, other images of other individuals will be obscured before the data is released.

For further information on subject access requests, refer to the ICO's 'Subject Access Code of Practice' https://ico.org.uk/media/for-organisations/documents/1065/subject-access-code-of-practice.pdf.

10.3 Freedom of Information

Trinity School may receive requests under the Freedom of Information Act (FOIA). We have a member of staff who is responsible for responding to freedom of information requests, and understands the school's responsibilities. We must respond within 20 working days from receipt of the request.

Section 40 of the FOIA contain a two-part exemption relating to information about individuals. If we receive a request for surveillance system information, we will consider:

- Is the information personal data of the requester? If so, then that information is exempt from the FOIA. Instead this request should be treated as a data protection subject access request as explained above in Section 10.2.
- Is the information personal data of other people? If it is, then the information can only be disclosed if this would not breach the data protection principles.

In practical terms, if individuals are capable of being identified from the relevant surveillance system, then it is personal information about the individual concerned. It is generally unlikely that this information can be disclosed in response to a freedom of information request as the requester could potentially use the information for any purpose and the individual concerned is unlikely to expect this. This may be unfair processing in contravention of the DPA.

11. Breaches of the Procedures (including security breaches)

- Any breach of these procedures by school staff will be initially investigated by the Head teacher, in order for him/her to take the appropriate disciplinary action.

- Any serious breach of the procedures will be immediately investigated and an independent investigation carried out to make recommendations on how to remedy the breach.
- Information obtained in violation of these procedures may not be used in a disciplinary proceeding against an employee of the school, or a student.

12. Monitoring and Review

Routine performance monitoring, including random operating checks, may be carried out by the Co-Headteachers, ICT Services Manager.

These procedures will be regularly reviewed, either by a designated individual within the school or by a third party. This is to ensure the standards established during the setup of the system are maintained.

Similarly, there will be a periodic review, at least annually, of the system's effectiveness to ensure that it is still doing what it was intended to do. If it does not achieve its purpose, it should be stopped or modified. Refer to **Appendix A** for a sample Annual Review Checklist.

The review will take into account the following:

- Is it addressing the needs and delivering the benefits that justified its use?
- Is information available to help deal with queries about the operation of the system and how individuals may make access requests?
- Does the information include our commitment to the recommendations in the ICO Code of Practice and include details of the ICO if individuals have data protection compliance concerns?
- Is a system of regular compliance reviews in place, including compliance with the provisions of the ICO Code of Practice, continued operational effectiveness and whether the system continues to meet its purposes and remains justified?
- Are the results of the review recorded, and are its conclusions acted upon?

The periodic review will also ensure all information is sufficiently protected to ensure that it does not fall into the wrong hands. This will include technical, organisational and physical security. For example:

- Sufficient safeguards are in place to protect wireless transmission systems from interception.
- The ability to make copies of information is restricted to appropriate staff.
- There are sufficient controls and safeguards in place if the system is connected to, or made available across, a computer, e.g. an intranet.
- Where information is disclosed, it is safely delivered to the intended recipient e.g. by Royal Mail Special Delivery if posted or identification verified and receipt signed for if collected in person.
- The Control room and room where information is stored is secure.
- Staff are trained in security procedures and there are sanctions against staff who misuse surveillance system information.
- Staff have been made aware that they could be committing a criminal offence if they misuse surveillance system information.
- The process for deleting data is effective and being adhered to.
- If there been any software updates (particularly security updates) published by the equipment's manufacturer that they have been applied to the system.

13. Complaints

- Any complaints about the school's CCTV system should be addressed to the Head teacher.
- Complaints will be investigated in accordance with Section 11 of these Procedures.

14. Further Information

Further information on CCTV and its use is available from the following:

- The Information Commissioners Office 'In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Data, May 2015 https://ico.org.uk/media/1542/cctv-code-of-practice.pdf
- The Information Commissioners Office (ICO) Website https://ico.org.uk/
- Information Commissioner's Office 'Conducting Privacy Impact Assessments' Code of Practice https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf
- Information Commissioner's Office 'Subject Access Code of Practice' https://ico.org.uk/media/for-organisations/documents/1065/subject-access-code-of-practice.pdf.
- Regulation of Investigatory Powers Act (RIPA) 2000 http://www.legislation.gov.uk/ukpga/2000/23/contents
- Data Protection Act 1998 http://www.legislation.gov.uk/ukpga/1998/29/contents
- The School/Setting Data Protection Policy

THIS PAGE IS INTENTIONALLY BLANK FOR PRINTING PURPOSES.

ANNUAL REVIEW OF CCTV SYSTEMS

This CCTV system and the images produced by it are controlled by Trinity School who is responsible for how the system is used and for notifying the Information Commissioner about the CCTV system and its purpose (which is a legal requirement of the Data Protection Act 1998).
Trinity School has considered the need for using CCTV and have decided it is required for the prevention and detection of crime and for protecting the safety of staff and students. It will not be used for other purposes. We conduct an annual review of our use of CCTV as follows.

School/Setting:		**Date:**	
Assessor:		**Signed:**	

	Satisfactory		**Problems Identified** *(if any)*	**Corrective Action Taken** *(if relevant)*	**Completed By**	**Date Complete**
	Yes	**No**				
Notification has been submitted to the Information Commissioner and the next renewal date recorded.						
There is a named individual who is responsible for the operation of the system.						
The problem we are trying to address has been clearly defined and installing cameras is the best solution.						
The CCTV system is addressing the needs and delivering the benefits that justified its use.						
A system has been chosen which produces clear images which the law enforcement bodies (usually the police) can use to investigate crime and these can easily be taken from the system when required.						
Cameras have been sited so that they provide clear images.						
Cameras have been positioned to avoid capturing the images of persons not visiting the premises.						
There are visible signs showing that CCTV is in operation. Where it is not obvious who is responsible for the system contact details are displayed on the sign(s).						
Information is available to help deal with queries about the operation of the system and how individuals may make access requests.						

	Satisfactory		Problems Identified *(if any)*	Corrective Action Taken *(if relevant)*	Completed By	Date Complete
	Yes	No				
Sufficient safeguards are in place to protect wireless transmission systems from interception.						
There are sufficient controls and safeguards in place if the system is connected to, or made available across, a computer, e.g. an intranet.						
Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them.						
The ability to make copies of information is restricted to appropriate staff.						
The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated.						
The process for deleting data is effective and being adhered to.						
Except for law enforcement bodies, images will not be provided to third parties.						
The potential impact on individuals' privacy has been identified and taken into account in the use of the system.						
The organisation knows how to respond to individuals making requests for copies of their own images. If unsure the controller knows to seek advice from the Information Commissioner as soon as such a request is made.						
Where information is disclosed, it is safely delivered to the intended recipient e.g. by Royal Mail Special Delivery if posted or identification verified and receipt signed for if collected in person.						
Staff are trained in security procedures and there are sanctions against staff who misuse surveillance system information.						
Staff have been made aware that they could be committing a criminal offence if they misuse surveillance system information.						
Regular checks are carried out to ensure that the system is working properly and produces high quality images.						

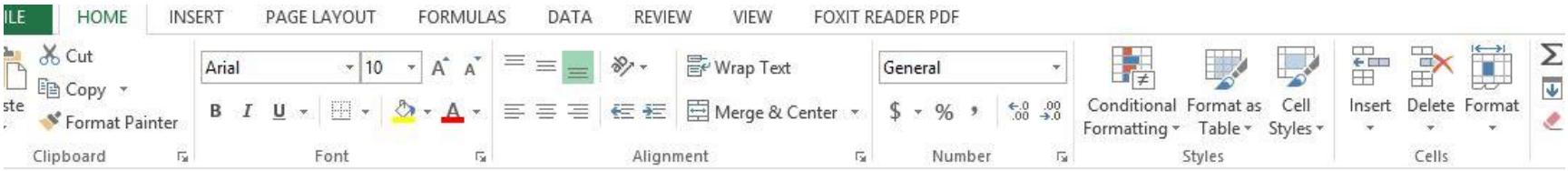
	Satisfactory		Problems Identified *(if any)*	Corrective Action Taken *(if relevant)*	Completed By	Date Complete
	Yes	No				
If there been any software updates (particularly security updates) published by the equipment's manufacturer that they have been applied to the system.						
Please keep this checklist in a safe place until the date of the next Annual Review.						

THE GUIDING PRINCIPLES OF THE SURVEILLANCE CAMERA CODE OF PRACTICE

System operators should adopt the following 12 guiding principles:

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.
7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.
8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.
11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.
12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

Source: *The Information Commissioners Office 'In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Data, May 2015 (Appendix 3)*



A	B	C	D	E	F	G
Date	**Operator**	**DVD / Photo**	**Incident**	**Date of Incident**	**Request Made By**	**Collected By**
01/11/1990	SSM	DVD	Bike taken from Bikesheds	29/10/1990	Cumbria Police	PC 999