Todwick Primary School CCTV Policy and Risk Assessment

September 2023

Todwick Primary School sets out to comply with the Data Protection Act (DPA) 1998 and CCTV Code of Practice 2008 where it uses CCTV systems. This policy statement and the following guidance must be complied with at all times on all Todwick Primary School premises.

1. Management must ensure that there is reasonable justification before CCTV is used.

2. On larger schemes, an assessment of impact on people's privacy must be undertaken. On smaller schemes the CCTV must not invade neighbour's privacy when viewing perimeter fencing.

3. A designated person will have legal responsibility of the scheme (Data Controller).

4. The intended use of the CCTV will be documented and the system must not be used for anything other than this. For example, if the scheme is merely for site security (viewing perimeters) then images of individuals must not be taken.

5. The scheme must be notified to the Information Commissioners Office (ICO). *update the ICO confirmed under our registration we do not need to inform them that we have CCTV.

6. Each system must have procedures for administration, which will include:

Ensuring notification on an annual basis.
Ensuring the scheme is in accordance with the notification.
Procedures for handling images.
Record keeping of access requests,
use of images procedures and Pro-active monitoring of the scheme to ensure compliance.
Control of recorded material.

7. The CCTV system must be sited only to achieve what is documented in the scheme.

8. Permanent or movable cameras must not be used to view areas that are not of interest and not intended to be the subject of the scheme. There are areas where there is an expectation of heightened privacy and CCTV may only be used in very extreme cases and this must not be undertaken without correct notification to the ICO and senior manager of the site (Head teacher / Building Managers at schools for example).

9. The CCTV will only be used at relevant times; times when site security is at risk for example.

10. The equipment used must be maintained to give reliable quality.

11. No sound recording technology is to be used.

12. Material must not be stored for longer than is necessary and must be deleted as soon as possible. For example, as soon as it is obvious that no crime has occurred, then the data must not be kept.

13. Images must be viewed in a secure/restricted area with access only to authorised persons.

14. Images must not be released to third parties. Police may legitimately request images.

15. Individuals who are recorded may request access to the images.

16. There must be adequate signage to let people know that surveillance is taking place. Where cameras are discreet, the notices must be more prominent.

17. The CCTV systems must not be used to systematically monitor people. If this is required to obtain the information that is needed, then authorisation under Regulation of Investigatory Powers Act (RIPA) 2000 will be required.

18. The scheme must be reviewed regularly by a local CCTV committee, to ensure compliance with the law.

19. A log is kept of viewage of CCTV, who has viewed it and reasons for the view.

All staff that use the CCTV must be trained and aware of this policy statement, the Data Protection Act 1998, the CCTV Code of Practice 2008 and the guidance developed by Todwick Primary School.

Introduction

1. Closed Circuit Television (CCTV) is now a well-established and accepted practice in our lives. It is widely used in towns, shopping areas, hotels, schools and on the road networks. CCTV is generally supported by the public, but it does intrude into people's lives as they carry out their daily activities. This therefore means that responsible use, under guidelines, must be maintained to ensure that this 'intrusion' is legitimately carried out.

2. A code of practice for CCTV was issued in 2000 by the Information Commissioners Office (ICO) and this has since been replaced by the 2008 revised edition. The 2008 edition strengthens the 2000 code by taking into account the advancement of technology. The code is available at:
www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_cctvfinal_2301.pdf

3. The code has been developed to ensure operators of CCTV systems follow good practice guidelines and comply with the law, in particular the Data Protection Act 1998 (DPA). Information about individuals (including images) that is held by any organisation, including local authorities, is covered by the DPA. The DPA has a number of **principles**, which are legally enforceable and are briefly included within this document (refer to Rotherham Metropolitan Borough Council's Data Protection policy for full details).

What is covered by the Code of Practice?

4. The 2008 code of practice covers CCTV systems which capture images of identifiable individuals, or information relating to individuals.

5. There are certain cases where the DPA is not applicable. These include:
• Householders who have CCTV for domestic use, e.g. to protect their properties.

• Images captured by individuals for personal (domestic) use on digital camera, mobile phones or camcorders.

6. Please note that any directed surveillance for law enforcement purposes is covered by the Regulation of Investigatory Powers Act (RIPA) 2000 and may require authorisation (contact Legal Services for further details).

When to use CCTV

7. Prior to installing a CCTV system, which must comply with the DPA, you must consider whether it is necessary or whether there is an alternative solution. For example, if the CCTV is purely for security, improved fencing and lighting may be a better option and won't require compliance with the DPA.

8. The code requires organisations to conduct an assessment before installation, to establish the following:
• Who is legally responsible for the system?

• What will the system be used for and how will it benefit the organisation?

• Can other, less intrusive, alternatives be used, such as lighting or improved fencing?

• Does the scheme capture images of identifiable individuals?

9. The Information Commissioner's Office states that if you are establishing a large system or considering a use of CCTV which could give rise to significant privacy concerns you may wish to consider using its Privacy Impact Assessment handbook.
http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html

Guidance for Schools

10. CCTV is an established part of everyday life and a proven tool in the fight against bullying, vandalism, graffiti and theft. One of the most rapidly expanding areas of use is in the education sector. CCTV is often used for surveillance in schools to prevent crime. Often, cameras are positioned to protect school premises and the general fabric of the building which helps to deter unwanted intruders from entering the school's perimeter. This has been particularly useful during school closures or holidays. Recently, there has been an increase in the use of CCTV not only for the purpose of protecting the school but for the intention of monitoring pupils and staff for the purposes of health and safety. This emerging trend has raised serious concerns within education circles claiming that this type of surveillance is an infringement of privacy laws.

11. Careful consideration should always be given to whether to use CCTV in the first instance; the fact that it is possible, affordable or has public support should not be the primary motivating factor. Schools should take into account what benefits can be gained and whether alternative solutions exist, and what effect it may have on individuals.

12. It would be strongly advisable to consult with staff, Governors, pupils and parents before installing any kind of CCTV system. It is recommended that the data controlling officer conducts a full consultation with all relevant parties. The consultation should include an explanation of all the purposes for which the CCTV cameras are being, or have been, installed and confirmation that they comply with the law as described in this policy.

13. High-quality toilet blocks sited at the heart of schools and near staff areas, with better design can help to eradicate the requirement for CCTV cameras altogether.

14. If CCTV is to be used, privacy must be safeguarded by ensuring that cameras are not directed at cubicles or urinals and ideally are sited outside main entrances / exits to toilets and washrooms. There have been many protests recently against the use of toilet block surveillance by both pupils and parents claiming that it is 'a step too far'. However, some individuals have claimed that there should be nothing to fear as long as pupils and staff conduct themselves according to school policy and house rules regarding behaviour.

15. CCTV should always be used proportionally and with caution and where there are justifiable concerns that make it necessary for cameras to be fitted. Circumstances might be when persistent thefts have occurred or if it is suspected that persistent bullying is taking place. However, even in those circumstances, this should be time limited, proportional and all staff and pupils should be fully informed of the reason/s why the cameras are present.

16. Below is a list of situations where CCTV should not be used:
• Cameras should not be fitted in staff rooms unless required for security reasons when the rooms are not occupied. In this case, it should only be switched on during those periods.

• Schools must be careful not to include captured images of surrounding properties and gardens, as this will contravene data protection regulations.
• In no circumstances should CCTV be placed in such a way that it could capture images of pupils changing.

Legal Issues
19. CCTV images, videos and webcams of clearly identifiable people will be subject to the DPA and the Human Rights Act 1998 and must be dealt with in accordance with these Acts.

Compliance with the Human Rights Act
20. The Human Rights Act 1998 (HRA) gives individuals the right to respect for their private and family life, home and correspondence. Public authorities may not interfere with this right except where necessary and in accordance with the law, in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. In practice, this means that authorities can use CCTV but only after they have risk assessed the impact on others privacy, whether the scheme is necessary, and for what purpose the images will be used.

Compliance with the Data Protection Act
21. **Principle 1** of the DPA requires that personal data is processed fairly and lawfully, i.e. that individuals are aware that images are being captured on CCTV, and of how that information will be used.

22. This means that signs, which are clearly visible and legible, should be displayed so that the public are aware they are entering an area where CCTV is in use. The signs should display details of the organisation responsible for the scheme, their contact details and the purpose of the CCTV system.

23. To ensure that images are only captured for the intended purpose of the scheme, the location of cameras must be carefully considered.
• The CCTV should be used only to monitor the intended spaces.

• Owners and residents of domestic premises should be consulted if domestic premises border the intended area to be viewed.

• Those operating the system must be fully trained, must be aware of what the scheme should be used for, and must only use the cameras and images for that purpose.

24. **Principle 2** requires that personal data be obtained for a specific purpose. Therefore, if you install CCTV for security purposes you would normally 8

only use that information for that purpose and wouldn't use it, for example, for staff monitoring.

25. Principle 2 also requires an organisation to notify to the Information Commissioner the purposes they process data for. If you use a CCTV system which will obtain personal information (i.e. images of individuals), you must ensure that your notification to the ICO includes this. Please note that all Council departments will be covered by the Councils notification which includes the purpose of processing information for crime prevention, safety and security. Other organisations (such as schools), which are a separate legal entity, will not be covered by the Council notification and must ensure they have their own notification in place.

26. **Principle 3** of the DPA requires that personal data should be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. This means that you should only collect the amount of data you need for the purpose the CCTV system has been installed for. You should collect no extra information and you need to ensure that the images will be adequate for their intended use.

27. **Principle 4** of the DPA requires that information should be accurate and up to date. The quality of images must be maintained to ensure that data within them is accurate and adequate for the intended purpose. In order to achieve this:
 Equipment should be maintained, serviced and cleaned regularly to ensure it performs correctly and a maintenance log should be kept.

• Tapes (if used) / discs should be of good quality and should be updated when necessary.

• If the system records location of camera, date, time etc. these should be accurate.

• Cameras should be protected from vandalism or tampering.

28. **Principle 5** of the DPA requires that information is held no longer than necessary for the intended purpose. Once a retention period has expired, images must be erased.

29. **Principle 6** of the DPA gives individuals certain rights under the Act. Section 7 of the DPA gives individuals the right of access to any personal data an organisation holds about them. This includes CCTV images and they have a right to view those images or request a copy.

30. A standard subject access request form is available on request from the school. 9

31. If individuals request CCTV images they should be asked to complete the form and provide any necessary identification (see the form for further details).

32. **Principle 7** of the DPA requires that information is held securely. Access to images, monitors and equipment should be by authorised staff only and copies of images should be stored securely.

Disclosure of CCTV Images

33. Access to, and the disclosure of, CCTV images and the disclosure of images to third parties should be restricted and carefully controlled to ensure the rights of individuals are protected.

34. All access should be documented (whether information is provided or refused), and disclosures must be limited to those allowed by law.

35. **Principle 8** of the DPA requires that information is not transferred outside the European Economic Area unless certain criteria are met. Take advice from Legal Services if any images are requested from any organisation outside of this area.

Compliance

36. To ensure compliance with the above requirements, please complete the user checklist (Appendix A) and CCTV Policy document (Appendix B) and forward to the Data Protection Officer, Legal Services, Doncaster Gate, Rotherham.

Advice

37. For further advice, please contact the Data Protection Officer, Legal Services, Doncaster Gate, Rotherham.