NEYLAND COMMUNITY SCHOOL

CCTV POLICY

Introduction

1.1 Neyland Community School uses closed circuit television (CCTV) images to reduce crime and monitor the school buildings in order to provide a safe and secure environment for pupils, staff and visitors, and to prevent the loss or damage to school property.

1.2 The system comprises of a number of fixed cameras.

1.3 The system does not have sound recording capability.

1.4 The CCTV system is owned and operated by the county council, the deployment of which is determined by the school’s leadership team.

1.5 The CCTV is monitored centrally from the Reception Office by the administrative assistant.

1.6 The introduction of, or changes to, CCTV monitoring will be subject to consultation with staff and the school community.

1.7 The school’s CCTV Scheme is registered with the Information Commissioner under the terms of the GDPR 2016 and Data Protection Act 2018. The use of CCTV, and the associated images and any sound recordings, is covered by the GDPR 2016 and Data Protection Act 2018. This policy outlines the school’s use of CCTV and how it complies with the Act.

1.8 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 the CCTV Code of Practice. All employees are aware of the restrictions in relation to access to, and disclosure of, recorded images and sound.

2. Statement of Intent

2.1 The school complies with 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.

2.2 CCTV warning signs will be displayed clearly and prominently. Signs will contain details of the purpose for using CCTV.

2.3 The planning and design has endeavoured to ensure that the 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.

3. Siting the Cameras

3.1 Cameras will be sited so they only capture images relevant to the purposes for which they are installed (described above) and care will be taken to ensure that reasonable privacy expectations are not violated. The School will ensure that the location of equipment is carefully considered to ensure that images captured comply with the Data Protection Act.

3.2 The school will make every effort to position cameras so that their coverage is restricted to the school premises, which may include outdoor areas.

3.3 CCTV will not be used internally.

3.4 Members of staff should have access to details of where CCTV cameras are situated.

3.5 Buses and coaches used for educational visits may use CCTV and audio recordings. This is beyond our control.

4. Storage and Retention of CCTV images

4.1 Recorded data will not be retained for longer than is necessary. While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded.

4.2 All retained data will be stored securely.

5. Access to CCTV images

5.1 Access to recorded images will be restricted to those staff authorised to view them, and will not be made more widely available.
6. **Subject Access Requests (SAR)**

6.1 Individuals have the right to request access to CCTV footage relating to themselves under the Data Protection Act.

6.2 All requests should be made in writing to the Headteacher. Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified. For example, date, time and location.

6.3 The school will respond to requests within 40 calendar days of receiving the written request and fee.

6.4 A fee may be charged per request.

6.5 The school reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an ongoing investigation.

7. **Access to and Disclosure of Images to Third Parties**

7.1 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).

7.2 Requests should be made in writing to the Head Teacher.

7.3 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.

8. **Complaints**

8.1 Complaints and enquiries about the operation of CCTV within the school should be directed to the Head Teacher in the first instance.

**Further Information**

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

- CCTV Code of Practice Revised Edition 2008 (published by the Information Commissioners Office)
- [www.ico.gov.uk](http://www.ico.gov.uk)
- GDPR 2016 and Data Protection Act 2018
Appendix 1 CCTV Signage

It is a requirement of the GDPR 2016 and Data Protection Act 2018 to notify people entering a CCTV protected area that the area is monitored by CCTV and that pictures are recorded. The school is to ensure that this requirement is fulfilled.

The CCTV sign should include the following:
- That the area is covered by CCTV surveillance and pictures are recorded
- The purpose of using CCTV
- The name of the school
- The contact telephone number or address for enquiries.

Appendix 2 Data Protection Act

The GDPR 2016 and Data Protection Act 2018: Data Protection Principles

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
   (a) at least one of the conditions in Schedule 2 is met, and
   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.