Brookfields School CCTV Policy

1. Introduction

1.1 Brookfields 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 loss or damage to school property.

1.2 The system comprises of a number of fixed and dome cameras.

1.3 The system does not have sound recording capability.

1.4 The CCTV system is owned by the school and the deployment of which is determined by the school's leadership team. The system is maintained by Amalgamated and Centurion undertake monitoring.

1.5 The CCTV is monitored centrally from the office of the Maintenance Officer.

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

1.7 The use of CCTV, and the associated images, is covered by the General Data Protection Regulations (GDPR) 2018. This policy outlines the school's use of CCTV and how it complies with the regulations.

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 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 Code of Practice is published at:

https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

CCTV warning signs will be clearly and prominently placed at all external entrances to the school, including school gates if coverage includes outdoor areas. Signs will contain details of the purpose for using CCTV. In areas where CCTV is used, the school will ensure that there are prominent signs placed at both the entrance of the CCTV zone and within the controlled area.

2.2 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.

Siting the Cameras

2.3 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 GDPR.

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

2.5 CCTV will not be used in classrooms.

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

2.7 The use of CCTV is clearly outlined in the school's Privacy Notices and will be implemented in accordance with such.

3. Covert Monitoring

3.1 The school may in exceptional circumstances set up covert monitoring. For example:

i) Where there is good cause to suspect that an illegal or unauthorised action(s), is taking place, or where there are grounds to suspect serious misconduct;
ii) Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

3.2 In these circumstances authorisation must be obtained from a member of the senior management team.

3.3 Covert monitoring must cease following completion of an investigation.

3.4 Cameras sited for the purpose of covert monitoring will not be used in areas which are reasonably expected to be private, for example toilets.

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. All CCTV data will be retained in accordance with the school's Data Protection Policy.

4.2 All retained data will be stored securely, in line with the school's Data Security Policy.

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 GDPR.

6.2 All requests should be 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 1 month.

6.4 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. Right to erasure

Under Article 17 of the GDPR individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances.

When does the right to erasure apply?

Individuals have the right to have their personal data erased if:

- the personal data is no longer necessary for the purpose which you originally collected or processed it for;
- you are relying on consent as your lawful basis for holding the data, and the individual withdraws their consent;
- you are relying on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- you are processing the personal data for direct marketing purposes and the individual objects to that processing;
- you have processed the personal data unlawfully (i.e. in breach of the lawfulness requirement of the 1st principle);
- you have to do it to comply with a legal obligation; or
- you have processed the personal data to offer information society services to a child.

When does the right to erasure not apply?

The right to erasure does not apply if processing is necessary for one of the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;
- for the performance of a task carried out in the public interest or in the exercise of official authority;
- for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- for the establishment, exercise or defence of legal claims.

In the case of such a request the school would have to consider the request and respond to confirm whether or not they are able to comply with it. Within the school CCTV system all images are retained for approximately 30 days before being deleted automatically.

8. Access to and Disclosure of Images to Third Parties

8.1 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).

8.2 Requests should be made in writing to the Headteacher.

8.3 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.

9. Complaints

9.1 Complaints and enquiries about the operation of CCTV within the school should be directed to the Headteacher in the first instance.

9.2 Where a complaint is in relation to the security or retention of data, the school's Data Protection Officer will be made aware.

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
- Regulation of Investigatory Powers Act (RIPA) 2000
- General Data Protection Regulations (GDPR 2018)

This policy will be reviewed bi-annually.
Produced September 2018.