BURTON BOROUGH SCHOOL

# CCTV POLICY

| | | | |
|---|---|---|---|
| **Policy Reviewer** | Sarah McElduff | **Date of Review** | May 2018 |
| **Date Presented to Governors** | | **Date of Next Review** | May 2020 |

**This page intentionally left blank**

**Contents**



……

## 1. Aims

The purpose of this policy is to regulate the management, operation and use of the CCTV system at Burton Borough School.

## 2. Objectives

- To increase personal safety of staff, students and visitors and reduce the fear of crime (Safeguarding arrangements).
- To protect the school building and their assets.
- To support the Police in a bid to deter and detect crime.
- To assist in identifying, apprehending and prosecuting offenders.
- To protect members of the public and private property.
- To assist in managing the school.

## 3. General Data Protection Regulations and CCTV Standards

Burton Borough School has chosen to use CCTV (closed circuit television) in various areas across the school including all external entrances and identified areas within the building. The General Data Protection Regulations, Regulation of Investigatory Powers Act 2000 (RIPA) and CCTV Code of Practice issued by the Information Commissioner explains how CCTV systems should be used, so that schools and individuals can enjoy security and safety whilst ensuring that individual rights are upheld. Burton Borough complies with the Code and adopts good standards of practice which helps towards realising this objective.

Use of CCTV can be affected by a number of Acts including the General Data Protection Regulations, the Human Rights Act and the Regulation of Investigatory Powers Act (RIPA). Failure to comply with these Acts or the related codes would cause the school to be in breach of the Law, render any evidence as inadmissible or carry penalties for the school, as the CCTV user, or individual members of staff.

## 4. Key Staff

Key staff have been provided with the necessary induction in the use of the CCTV systems and only those members of staff have access to the recordings within the system.

Mr N. Wright (Site Manager)
Mr B. Evans (Assistant Site Manager)
Mr S. Attwood (ICT Manager)
Mr N. Maloney (Senior ICT Technician)
Mr J. Blakeway (ICT Technician)
Mrs P. Johnston (Cover Supervisor)

## 5. Scope of Use

The school has undertaken the following checklist to ensure that the CCTV system remains within the law and that images can be used for crime prevention.

- The school has specified that the CCTV cameras have been installed for the safeguarding of staff and students and for detection and prevention of vandalism across the school estate.
- Significant signage is found in prominent positions on the external entrances to the building that CCTV cameras operate to inform staff, students and the general public that they are entering an area where their images are being recorded either as still or video footage.
- The school retains the right to be the data controller for all footage recorded through the use of its CCTV cameras.
- The equipment is sited so that it only monitors those spaces that are intended to be covered by the equipment.
- All operators (staff who operate and monitor CCTV) are aware of the purposes for which the scheme has been established.
- Operators are aware that they are only able to use the equipment in order to achieve the purposes for which it has been installed i.e. safeguarding and the prevention and monitoring of vandalism.
- The images are stored on a secure server and the retention period is for 8 days.

## 6. Code of Practice

- This CCTV Policy will be reviewed every 2 years.
- The CCTV system is owned and operated by the school.
- The footage may only be viewed by authorised members of staff as listed above.
- Images required as evidence will be removed from the server and stored in a secure location.

## 7. Breaches of the Code

- Any breach of the code of Practice by the school will be initially investigated by the Principal, in order for them to take the appropriate disciplinary action.
- Any serious breach of the Code of Practice will be immediately investigated and an independent investigation carried out to make recommendations on how to remedy the breach.

The following Do's and Dont's as advised as part of the Data Protection Policy and are adhered to by the school.

## 8. Do

- Authorised Users update the CCTV Access Request Log each time a request to view footage is made.
- Ensure CCTV is the only viable option to achieve the stated purpose.
- Formally assess the appropriateness of and reasons for, using CCTV.
- Consult the relevant parties involved.
- Undertake regular reviews of both the use of the CCTV system and the procedures to ensure compliance with the law.
- Ensure that film / images are not kept for longer than necessary – at the moment the data retention is for 8 days.
- Process (working with, using, passing on data) images in a lawful manner.
- At the point of obtaining images provide:
- The identity of the data controller (name and address of school).
- The identity of the representative the data controller has nominated for the purposes of the Act.
- The purpose or purposes for which the images are intended to be used; and
- any information which is necessary, having regard to the specific circumstances in which the images are, or are to be, processed to enable processing in respect of the individual to be fair.
- Establish and document the person(s) who are responsible for ensuring day□to□day compliance with the requirement of the Code of Practice.
- Make certain there are procedures for dealing with police enquiries, i.e. access under the GDPR or removal of evidence under Police and Criminal Evidence Act.

- Where footage is requested by a third-party, sufficient checks are made by verifying identities and having written proof (eg. Police request) that the persons making the request, are authorised to do so. Detail should also be given how to identify the intended footage (eg. time of day, what person was wearing etc).
- Export video or images and store them in secure locations on the network and that only the intended recipient(s) receive them.

## 9. Don't

- Film areas that could amount to an infringement of personal privacy.
- Ignore subject access requests (an individual's written request to access information about themselves under the General Data Protection Regulations). A person identifiable on CCTV images may be entitled to view the footage and may make a request to do so.
- Use CCTV footage for any other purpose other than what it was originally used for e.g. Prevention and detection of a crime.
- Use covert (i.e. where it is calculated to ensure that the persons are unaware) monitoring without seeking legal advice.
- Use inadequate equipment. Blurred or indistinct images could constitute as inadequate data, whilst poorly maintained equipment may not provide legally sound evidence.
- Disclose data to third parties, unless it is lawful to do so.
- Systematically monitor people by use of CCTV.

## 10. Links with Other Policies

This CCTV policy is linked to our:

- Privacy Notice
- Data Protection policy
- Freedom of information publication scheme
- Data collection forms
- Home / school agreement
- Media agreement
- Staff handbook / acceptable use policy
- Records management policy