Surveillance Policy

Introduction

This policy is concerned with the use and governance of surveillance technology, and the processing of Personal Data which has been collected by using surveillance technology. The policy is written in accordance with various Data Protection legislation, which includes but is not limited to the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA), and the Information Commissioner's Office's (ICO) surveillance code of practice.

Queries about this policy should be directed to Bridgewater's Data Protection Officer.

Scope

This policy applies to all school employees (both those employed directly by the school and those employed on behalf of the school by a local authority or other such body), any authorised agents working on behalf of the School, including temporary or agency staff, governors, volunteers, and third party contractors.

This Policy will refer to all individuals within scope of the policy as 'employees'. Employees who are found to knowingly infringe this policy may face disciplinary action.

Surveillance is the monitoring of behaviour, activities, or other changing information for the purpose of influencing, managing, directing, or protecting people. The school only uses surveillance in the context of CCTV and e-monitoring software.

The school does not operate covert surveillance technologies and therefore this policy does not cover the use of such technology.

CCTV

The school operates 'Closed Circuit Television' (CCTV) systems in order to safeguard children and prevent / detect crime.

Our CCTV systems will employ the concept of 'privacy by design' which will ensure that privacy implications to data subjects will be considered before any new system is procured. The prescribed method for this is through the completion of a Data Protection Impact Assessment (DPIA).

The school has various statutory responsibilities to protect the privacy rights of data subjects. Therefore the school will always consider:

1. The purpose of the system and any risks to the privacy of data subjects,

2. That there are statutory requirements placed on the location and position of cameras. This means that cameras must be positioned to meet the requirement(s) of the intended purpose(s) and not exceed the intended purpose(s).

3. The obligation to ensure that the CCTV system can meet its intended purpose(s) also means that the system specification must be such that it can pick up any details required for these aims. For example the system must record with sufficient resolution to perform its task.

4. The system must also have a set retention period (the typical retention period is one month) and, where appropriate, the school must also have the ability to delete this information prior than the set retention period in order to comply with the rights of data subjects.

5. That the school will need a level of access to the system and there will need to be the option to provide other agencies (such as law enforcement agencies) with specific footage if requested. If a data subject is captured and recorded by the system, then that individual also has the right to request a copy of that footage under subject access provisions.

The school will ensure that a contract will be agreed between the school (as Data Controller) and the CCTV system provider. Consideration should also be given as to whether there are any joint data controller arrangements where the system is shared with another organisation.

CCTV Privacy Notices
The processing of personal data requires that the individuals that the data relates to (in this case any individuals captured by the CCTV) are made aware of the processing. Therefore the use of CCTV systems must be visibly signed.
The signage will include the purpose for the system (e.g. the prevention or detection of crime), the details of the organisation operating the system and who to contact about the system (including basic contact details). The signage must be clear enough that anyone entering the recorded area will be aware that they are being recorded.

A more detailed Privacy Notice for the use of CCTV must be maintained with the intention of informing data subjects of their rights in relation to surveillance data.

Access to CCTV Recordings
CCTV footage will only be accessed to comply with the specified purpose listed above.

The CCTV system will have a nominated Information Asset Owner who will be responsible for the governance and security of the system. The Information Asset

Owner will authorise officers to access CCTV footage either routinely or on an ad-hoc basis.

CCTV Footage Disclosures
A request by individuals for CCTV recordings that include footage of them should be regarded as a subject access request (SAR). For more information on the right of access for individuals captured on CCTV, refer to the School's Information Policy.

If the school receives a request from another agency (for example a law enforcement agency) for CCTV recordings, data will not be shared unless a warrant / court order is presented.

The School will liaise with its appointed Data Protection Officer should it have any concerns about such requests.

Review of CCTV
CCTV systems must be reviewed biennially to ensure that systems still comply with Data Protection legislation and national standards. The Information Asset Owner should use the checklist included in Appendix 1 of this policy to complete this review. It is the responsibility of the Information Asser Owner to ensure reviews are completed and evidence of those reviews taking place are maintained.

Complaints

Complaints by individuals about the use of surveillance systems, or the way surveillance data is processed, should be treated as a data protection concern and the school's data protection officer should be made aware.
The School's Data Protection Officer is:

Information Governance
Veritau Ltd
County Hall
Racecourse Lane
Northallerton
DL7 8AL

schoolsDPO@veritau.co.uk
01609 53 2526

Records of Processing

The school has a duty under Article 30 of the GDPR to ensure that all instances of data processing activity is recorded for regulatory inspection where required. The school maintains an information asset register in order to fulfil this requirement.

The school will ensure that the use of surveillance systems is recorded on their information asset register. This should detail each separate surveillance system in use.

Related Documents

Employees who are responsible for planning, maintaining, or reviewing the implementation of a surveillance system are encouraged to read the following related documents prior to implementation:

- ICO Surveillance Code of Practice (External Link)
- The School's Data Protection Impact Assessment (DPIA) Template (available through Veritau)

Review

Agreed: May 2019

Review Date: Summer 2020

Appendix 1 – Surveillance System Checklist

School Name:

Name and Description of Surveillance System:		
The purpose and requirements of the system are addressed by the system (i.e the cameras record the required information)	**YES**	**NO**
	Notes:	
The system is still fit for purpose and produces clear images of adequate resolution.	**YES**	**NO**
	Notes:	
Cameras are sited in effective positions to fulfil their task.	**YES**	**NO**
	Notes:	
Cameras are positioned so that they avoid capturing the images of persons not visiting the premises and/or neighbouring properties.	**YES**	**NO**
	Notes:	
There are visible signs showing that CCTV is in operation. These signs include: ▪ Who operates the CCTV, ▪ Their contact details, ▪ What the purpose of the CCTV is.	**YES**	**NO**
	Notes:	
CCTV recordings are securely stored and access limited.	**YES**	**NO**
	Notes:	

The system has the capability to transfer recordings to law enforcement or to fulfil a request for an individual's own personal information.	**YES**	**NO**
	Notes:	
The system has a set retention period. This retention period should only be long enough to fulfil the CCTV's purpose and not longer. Outside of this retention period information should be deleted	**YES**	**NO**
	Notes:	
The system users should be able to selectively delete information still inside the retention period to fulfil the right to erasure.	**YES**	**NO**
	Notes:	
All operators have been authorised by the Information Asset Owner and have sat their mandatory data protection training.	**YES**	**NO**
	Notes:	
This system has been declared on the corporate register of surveillance systems.	**YES**	**NO**
	Notes:	

Checklist Completed By: Name: Job Title: Date:	**Checklist Reviewed and Signed By (Information Asset Owner):** Name: Job Title: Date: