Surveillance Policy

Document History	
Created or reviewed:	22.08.23
Reviewing officer:	SBM
Review frequency:	2 yearly
Review date:	22.08.25

Version Control			
Version	Date	Notes and amendments	Approval
0.1	22.08.23	Adapted from Veritau template	SFP

Surveillance Policy

Introduction

This policy concerns our use of surveillance technology and related processing of personal data. It is written in accordance with data protection and human rights legislation and relevant codes of practice.

Surveillance is the close observation or monitoring of individuals or spaces, for the purpose of influencing behaviour or protecting people. We only use surveillance in the context of e-monitoring software. We do not operate covert surveillance technologies and therefore this policy does not cover the use of such technology.

E-monitoring

We operate e-safety monitoring software systems to:

- Safeguard our pupils and staff
- Promote wellbeing and early intervention
- Ensure appropriate use of school assets and resources
- Monitor compliance with school rules and policies
- The school uses Smoothwall (via CYC)

Privacy Risk Assessment

Under the UK GDPR, we are required to consider and address privacy implications to data subjects when implementing new data processing systems. This is known as privacy by design. The usual method for assessing privacy risks to individuals is by carrying out a Data Protection Impact Assessment (DPIA).

A DPIA is mandatory for surveillance activities since they are deemed particularly intrusive. We will ensure that DPIAs have been completed for e-monitoring and that there are no unmitigated high risks to the rights and freedoms of data subjects. In addition, we will review and update the relevant DPIA if we substantively change our systems.

Contract Management

We are required to have contracts with any data processors we use, containing certain data processing clauses prescribed by law. We will ensure that we have implemented an appropriate contract with the providers of our e-monitoring systems to allow for them storing, monitoring or accessing the data on our behalf. We will only agree to these contracts where they have been assessed for compliance and determined to meet our requirements.

Transparency

The use of e-monitoring systems must also be clearly signed. Users will be made aware of the e-monitoring by a notice on the log in screen of computers and/or on the browser page when they join the network.

More detailed information about use of e-monitoring must also be provided via a Privacy Notice, which must also inform data subjects about their rights in relation to their surveillance data. We have included the mandatory privacy information to data subjects in our relevant privacy notices.

Access Controls

Surveillance system data will only be accessed to comply with the specified purpose.

Each system will have proportionate access controls and a nominated Information Asset Owner (IAO) who will be responsible for the governance and security of the system. The IAO may authorise other specified staff members to access data held on the systems routinely or on an ad-hoc basis.

Disclosures

A request by an individual for surveillance data held about them will be treated as a subject access request (SAR). For more information on data subjects' right of access to their information, please refer to our Data Protection Policy.

If we receive a request for surveillance data from an official agency, such as the police, then we will confirm the purpose of the request and their lawful basis for accessing the data. We may also require formal documentation in support of the request. We will liaise with our Data Protection Officer (DPO) if we have any concerns about such requests.

Record of Processing and Retention

We have a duty under Article 30 of the UK GDPR to ensure that all our data processing activities are recorded for accountability purposes. We maintain an Information Asset Register to fulfil this requirement. We will ensure that the use of surveillance systems is detailed on this register.

Surveillance records will only be held as long as necessary to fulfil the specific purpose and deleted in line with our Records Management Policy.

Reviews

The school should review the e-monitoring systems regularly by undertaking a review of the DPIA and updating the DPIA to reflect any changes in how the system is used or the type of data that is collected.

It is the responsibility of the relevant IAO to ensure reviews are completed and evidence of this is maintained.

Complaints

Complaints by individuals about the use of surveillance systems or data will be treated as a data protection concern. For more information on data protection complaints, refer to our main Data Protection Policy.