SUTTON VALENCE SCHOOL
SINCE 1576

Electronic Communications Policy

(Prep School and Senior School)

Author: Mr Glen Millbery
Policy review date: September 2025
Approval date by Governors: November 2025
Review Date: September 2026

This Policy applies to Sutton Valence School (including as the context requires, the Nursery, the Prep School and Senior School).

Policy for the Use of Electronic Communications

Introduction
This policy is based on the Data Protection Code guidelines for Employment Practices. It ensures that all monitoring is in accordance with the GDPR, KCSIE, The Regulation of Investigatory Powers Act and the Lawful Business Practice Regulations.

Monitoring is a recognised component of the employment relationship and is standard for organisations. Most employers will make some checks on the quantity and quality of work. This monitoring includes looking at marked work and observation of lessons.

Within the workplace, monitoring is expected. It is there to safeguard employees as well as to protect the interests of the School, the pupils, the parents and visitors.

Where monitoring goes beyond one individual watching another and involves the manual recording or any automated processing of personal information, it must be done in a way that is both lawful and fair to employees, pupils, parents and visitors.

Use of Email, Telephone and Internet
Staff at Sutton Valence School are provided with email, telephone and internet facilities to assist them with their jobs. This might entail:

- looking for documents, information and worksheets;
- making telephone calls;
- messaging;
- video conferencing;
- engaging in newsgroups and discussion groups.

The nature of Sutton Valence School is such that staff are allowed to make use of the facilities at the discretion of the Headmaster for personal use.

This use of email, telephone and internet facilities for personal use is a privilege and not a right and can be removed.

If a member of staff does not wish their personal emails, telephone calls and internet sites to be viewed or monitored then they should not use the School system.

Use of CCTV
CCTV is used both outside and within buildings at Sutton Valence School. The CCTV is recorded and there is a live feed to monitors. Access to CCTV footage is restricted to specific staff who require it as part of the fulfilment of their contract and must follow the occasional monitoring procedures to view it.

CCTV/Lesson Recordings in classrooms
Recordings that are made in SVS classrooms can include CCTV or the use of appropriate lesson recording software.

Recordings may be made by the teacher to assist with absent pupils or staff training. Pupils and staff will be notified that the lesson is being recorded.

Recordings that are made as part of distance learning will initially be stored on the members of staff laptop (a school owned device) and uploaded to the server as soon as is possible. This recording will then be deleted from the laptop.

Recordings of lessons will be accessible by those that were present in the recording via a link and those members of the class that were absent. The recording can also be accessed by members of staff to assist with teaching practice, observation of lessons and investigation into any complaints.

Viewing of lesson recording is not part of monitoring unless it is part of a complaint or investigation in which case the monitoring process below must be followed.

Extent and Type of Personal Use
Personal use is defined as any use that is not related to the job. If you use the School facilities for personal use, then it is subject to the same monitoring methods that are applied to School use.

However, not all personal use is acceptable on the School network. There are restrictions on the types of material that can be viewed. The School has a filtering system in place and any sites that are filtered cannot be viewed. If the material is offensive in words and/or imagery or inappropriate for and damaging to the School as deemed by the Headmaster, then it is not suitable for viewing using the School equipment.

There is a general need to exercise care. The staff are in a position of trust and need to be aware of what they are doing. This includes what they are viewing on the internet and the content of emails.

Purpose of Monitoring
The purpose of monitoring is to protect the organisation and the individuals within the organisation – the employees and the students.

The School has a business responsibility to protect its information. This includes information necessary for the running of the School. The School also has a responsibility to protect the equipment and individuals within the School. Monitoring can assist in these roles.

Forms of Monitoring
There are two main forms of monitoring – systematic and occasional.

1. Systematic monitoring is where all employees and pupils are monitored as a matter of routine;
2. Occasional monitoring is where monitoring is introduced as a short-term measure in response to a particular problem or need.

Sutton Valence School makes use of both types of monitoring.

Systematic Monitoring
Whenever a user logs onto the School system and makes use of electronic communications, all activity is logged. This activity includes (depending on the service used):

- Who is using the internet;
- Which PC they were using;
- When they are using it and how long they were on the site for;
- Which web pages they are viewing and files downloaded;
- Keywords entered;
- The phone number dialled and duration of the call.

School owned devices and any personal devices that connect to the School's network are systematically monitored and filtered by Smoothwall in line with requirements by KCSIE. School owned devices and those on the Easy4U scheme are also monitored and filtered off site. Breaches detected by the automated Smoothwall filtering system or monitoring are escalated to the Designated Safety Lead or Headmaster.

All images stored on the School network are also filtered for content.

Systematic monitoring also occurs with emails. This is done by the use of software to automatically scan emails for pre-set words and phrases. Points are awarded for violations and when a certain number of points is reached the email is automatically deleted. A message is then sent to the sender giving reasons why the email has not been sent.

Systematic monitoring is also conducted using Microsoft in built tools for personal data and financial information. If an email is in violation of the rules, a warning is sent to the Data Compliance Officer with the email subject, names of any attachments and the rules that have been broken (the contents of the email are NOT included). Based on the information the email may be tracked and the sender informed.

The CCTV security cameras located around the School are involved in systematic monitoring. The record is based on movement and automatically stored on the School servers.

These processes are completely automated, there is no human intervention.

If the items being monitoring (screen viewed, keystrokes) meets a pre-determined threshold it is referred to moderators at Smoothwall who will contact the School DSL.

Occasional Monitoring
Occasional monitoring is the deliberate targeting of websites, files, video footage and looking at emails sent and received by an individual, Teams messages and any other school system which logs information.

Occasional monitoring needs to be authorised before it can be carried out.

The individual may or may not be notified that occasional monitoring is taking place.

Occasional monitoring will only take place where there are grounds for suspecting criminal activity or equivalent malpractice, contravention of the school's policies or a legal requirement, such as a subject access request, or preparation for a subject access request. Occasional monitoring of students can take place where there are grounds for believing that School rules have been broken or for safeguarding purposes.

All occasional monitoring must be preceded by authorisation. Authorisation in the case of Safeguarding can be the Safeguarding Lead but for all other cases it needs to be the Data Compliance Officer, Headmaster or Chair of Governors. The individual giving authorisation cannot be the same as the individual requiring access.

In order to conform to GDPR, if occasional monitoring has taken place a record must be made. This record forms part of the material which can be requested by a member of staff or student along with other information stored on them under the requirements of GDPR.

In monitoring of emails, for example in response to a SAR, it is likely that emails sent/received by individuals who have not requested the SAR will be included and examined.

It is not anticipated that the School will undertake occasional monitoring of staff. If it does take place, then it will be a very rare occurrence. Occasional monitoring of students is likely to be more widespread.

Occasional monitoring, once authorised can be carried out but must involve more than one person viewing the results.

Occasional monitoring is logged on a form accessible through the staff area of the portal.

Covert Monitoring
Covert CCTV monitoring is where the device used to monitor is not visible. This may be the use of a device that contains a camera, such as a clock. It is deliberately intended to mislead the individuals being monitored, so that they do not know that they are being monitored.

This is to be used in exceptional circumstances, such as vandalism.

The attached form – Use of Covert CCTV Monitoring - needs to be completed BEFORE the monitoring begins and must be reviewed and agreed by a senior member of staff or a governor.

There must be a timescale put in place before monitoring begins and if it needs to be extended, another form completed.

If the footage is to be reviewed, then Monitoring form must be completed.

Use of Covert CCTV Monitoring

Date	

Requested by:	

What is the purpose of the monitoring?

How long will the monitoring be in place for?

Why does the monitoring need to be covert?

Is the monitoring likely to capture images of "innocent" pupils and staff? How will this footage be used?

Reviewer Comments

Date	

Reviewed and agreed by:	