SEVENOAKS
PREPARATORY SCHOOL

Information Technology Monitoring Privacy Notice

Status and Review Cycle	Non-statutory / Annual
Policy reviewed and amended	28.02.2024
Next review date	28.02.2025
Governor Lead	
Policy Holder	Elizabeth Walsh bursar@theprep.org.uk Liam Rogers liam.rogers@theprep.org.uk

What is the purpose of IT monitoring and filtering?

Sevenoaks Preparatory School is committed to ensuring it provides a safe environment for children to learn in, identifies children who are suffering, or likely to suffer, significant harm and takes appropriate action to see that such children are kept safe, both at home and at school.

This commitment requires that we take measures to prevent children in our care from accessing unsuitable or harmful material online, and to take action if access to such material is detected on-site. The school is legally required under the government's statutory guidance, Keeping Children Safe in Education to have in place appropriate filtering and monitoring. In addition, according to the UK government's PREVENT strategy, attention must be paid to ensure that pupils are safe from terrorist or extremist material with appropriate levels of Internet filtering. In order to ensure that the school environment is safe, we extend some level of filtering and monitoring to all those using the school's Internet connection.

Some monitoring of pupils specifically is performed to detect misbehaviour in class or misuse of the IT system .

If there were significant concerns about the professional conduct or performance of a particular staff member, the IT monitoring systems may be checked for evidence of that concern.

Monitoring and filtering is also used for ensuring the security of the school IT system and protecting the sensitive and personal data that the school holds, by blocking malicious software and monitoring for attempts to subvert the security of the system.

Phone logs are used to monitor costs and detect unnecessary use of the phones.

What IT monitoring and filtering is in use on non-school devices?

All access to the Internet via the school's connection is monitored and filtered. This includes HTTPS secure webpages that would normally be kept private during transmission. Web pages are scanned automatically, and those detected as unsuitable, through methods such as key word detection, will be blocked.

All website addresses (URLs) visited, and text entered into web search engines are recorded for review by our safeguarding and online safety officers. Content sent to or received from the Internet may be used for automatic detection of unsuitable web pages or communication. However, content other than the page address is not recorded. Exceptionally, if necessary to diagnose a problem with the system or to counter or detect an attempt to subvert security measures, the content of non-secure internet communication may be temporarily stored and examined strictly for these purposes.

Access to certain sensitive websites, such as banking websites, may be whitelisted and permitted without the contents of messages being examined. However, the school's Internet connection is not intended for sensitive communication private from the school.

What IT monitoring and filtering is in use on school devices?

In addition to the internet monitoring and filtering described in the previous section, school computers usually have screen monitoring software installed. While devices are on the school site, this allows remote viewing of what is shown on the screen, however the image is not recorded unless a screen capture or recording is requested by the operator.

Logs are kept of calls made on school phones (including software phones) recording the time, number called and duration of call, but not the contents of the call. Recording of a call may be enabled by a staff member, but they must not do this without asking for the consent of the other party and prior authority from the bursar. Calls to some international numbers and premium rate numbers are disabled from most phones.

What is the purpose of the school's HTTPS inspection certificate?

Many webpages now use HTTPS protection to protect data during transmission. This protection also prevents our systems from effectively monitoring or filtering the webpages, so in order to fulfil our legal requirements we use HTTPS interception to bypass the protection.

Without the school's HTTPS inspection certificate installed, many web pages will display a warning when visited due to the inspection of the normally private connection. The inspection certificate is only installed on school owned devices. We advise not to visit web pages that show security warnings, as they may be monitored by someone other than the school.

How are monitoring records stored, processed and shared?

Access is strictly controlled to records of internet access and logs of website addresses visited. Access is limited to those staff and governors necessary to fulfil the purposes of safeguarding, staff management and system security; and to maintain the system. For most records, this is the online safety and safeguarding officers, bursar, headmaster and IT department staff.

Access to screen monitoring on school computers (not personal devices) is as follows:

- Teachers can view screens of pupils within their class or potentially adults if they use a pupil device.
- IT staff
    - Monitor pupils' screens sporadically to detect misuse of the IT system
    - May see thumbnail sized images of other screens, but view other's screens full size only if they have reasonable suspicion of a serious breach of professional conduct, or with the individual's permission for technical support purposes.
- Head and Bursar

- May monitor any screen occasionally as part of a random sweep for serious breaches of professional conduct or safeguarding concerns.
- Would not record or act on any information except in case of safeguarding concerns or serious breaches of professional conduct.
- May undertake longer term monitoring of a specific individual only if this is necessary for an investigation into such concerns.

Access to phone logs is limited to the IT department staff, head and bursary staff.

If evidence of a safeguarding concern is uncovered, then relevant records may be shared more widely with staff and governors needed to assist, such as a pupil's form teacher, and with external official safeguarding bodies such as the Kent County Council safeguarding officers. Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Kent Police or CEOP.

Other than this, these records are not shared or used for any other purposes within the school.

The security of the system is maintained and reviewed by the school's IT & Network Manager.

For how long are IT monitoring records stored?

Internet access records and phone call logs are retained for 1 year as active records and then approximately 1 year in archive backups. After this time, they are overwritten. If specific records provide evidence for a child safeguarding or HR investigation, they may be extracted and stored for longer (indefinitely for safeguarding, 7 years for HR).