

RESPONDING TO MONITORING SOFTWARE ALERTS PROCEDURE

Introduction and context

This procedure sets out how the college responds to alerts from our IT monitoring software, Smoothwall. These alerts are related to student and staff activity on college devices (on and off site) and are intended to flag potentially harmful or concerning activity.

This procedure sets out how we respond as part of our duty to safeguarding students whilst balancing this responsibility with respect for students' rights. It should be read in conjunction with our Safeguarding, Behaviour and Social Media and Online Safety policies.

Principles

Student Safeguarding: Alerts must be addressed to protect the wellbeing of students, particularly in cases involving harm, radicalisation, bullying or illegal activity.

Data Privacy and Security: Access to alert information should be restricted to those within the safeguarding team or staff with pastoral responsibility for the student(s). See the procedure set out below for information on who might be involved in responding to the alert.

Transparency: Students and staff have been informed about the monitoring process.

Proportionality: Responses should be proportionate to the concern raised and based on the information/screenshots which form part of the alert.

Procedure for Handling Alerts

Initial Review of Alert

1. An alert is generated by Smoothwall. It is a real-time, human moderated service and thus some context is generally provided with screenshots where possible.
2. Initially, this alert only comes to the DSL and DDSL. However, where a genuine safeguarding concern is identified, members of the safeguarding team might also be informed, particularly where we are able to identify trends in activity. In the case of alerts relating to staff, only the DSL/Assistant Principal for Student Experience is informed.
3. The DSL or DDSL reviews the alert, context and risk level Smoothwall has ranked it at. Low level alerts are stored in the software dashboard for viewing when convenient. Medium alerts are communicated through email. High alerts are conveyed by phone.
4. The DSL/DDSL identify if the alert requires immediate action (e.g., threats to safety).
5. The Smoothwall system automatically logs and stores the alert. This includes the date and time of alert, student details (ID number, name) and a description of the flagged activity.

Response

Having determined the context and/or severity of the alert, the DSL/DDSL will do the following:

Low level alert

- Likely to be a false positive (e.g., language out of context, such as media students using term 'shot' when referring to filming) or non-harmful curiosity.

Outcome/next steps: Will either be no further action and closed on the system or referred to either PDT/DTL/PTL for a conversation.

Student will be gently reminded of what constitutes acceptable use of college IT facilities if appropriate to do so.

Not logged on CPOMS or student tracking.

Medium level alert

- Not an immediate concern but in need of same day/ next day(s) follow up (e.g., enquiries or comments using terms that could be violence, drug or harm related, including general, not person specific discriminatory language or language with the potential to offend).
- Either PDT/PTL/DTL will contact the student to discuss it further and understand the context or the DSL/DDSL/safeguarding officer, where deemed appropriate.
- **Outcome/next steps:** Where there has been use of discriminatory language, the PTL will meet with the student and the result could be a three-week behaviour contract to provide further education/support relating to the issue.

Student will be reminded of what constitutes acceptable use of college IT facilities if appropriate to do so.

Where a support need is identified, college pastoral or counselling/student services team may offer further support.

There might be the need to gather information from other staff for additional insight into the student's recent behaviour/attendance/circumstances.

Parents/carers might also be informed depending on the nature of the language used or the alert content (unless this puts the student at greater risk).

Logged on CPOMS and a note to say there has been a Smoothwall alert on student tracking (without detailing the content).

High level alert

- Immediate risk to the safety of a student or others (e.g., evidence of desire to self-harm or harm others, suicide, weapons, illegal activities or the explicit use of discriminatory/hate language directly targeted towards an individual or group).
- DSL/DDSL/safeguarding officer will contact the student immediately on receipt of the alert to discuss it further and understand the context. This could involve taking the student out of a lesson.
- **Outcome/next steps:**

The student will be sought out immediately and the alert discussed between them and the DSL and/or DDSL, possibly with the safeguarding officer present.

If we cannot reach the student (on or off site) we may need to go directly to the next of kin.

There might be the need to gather information from other staff for additional insight into the student's recent behaviour/attendance/circumstances.

Parents/carers are highly likely to be informed depending on the nature of the language used or the alert content (unless this puts the student at greater risk).

Student will be reminded of what constitutes acceptable use of college IT facilities if appropriate to do so.

Where there has been use of discriminatory language the result could be a three-week behaviour contract to provide further education/support relating to this. It could also be determined that a serious breach of the code of conduct has occurred, and in such cases the college behaviour policy will need to be followed.

Where a support need is identified, college pastoral or counselling/student services team may offer further support.

It may be necessary to make a referral to an external specialist agency or organisation to safeguard the student or others. This could include contacting the emergency services.

Logged on CPOMS and a note to say there has been a Smoothwall alert on student tracking (without detailing the content).

Post-alert Actions

Documentation: Ensure all actions and decisions are logged on CPOMS and student tracking.

Follow-Up: Inform all necessary staff members and external agencies where appropriate. Arrange any follow-up meetings and support with the student and/or parents/carers.

Responding to alerts

Some college staff and a small number of students have devices that belong to Callywith to work on outside of college. As they are college property, the Smoothwall monitoring software is installed. It is therefore possible that an alert may be received outside of normal college hours.

Smoothwall alerts will be responded to during normal working hours. Therefore, were an alert to be received after 5pm, it is likely it will not be picked up until 8.30am on the next working day.