Monitor

Start-of-Year Maintenance Checklist

School / Organization

Name

Date

1. Check all devices

Note: This section should be completed by a **Safeguarding Contact**..

#	Action	Description	Done*	Notes
1.1	Check for inactive devices	Check the number of Devices in Monitor against the expected total. Compute the number of Devices running Monitor by adding the devices that: • Did not send any captures in over 7 days. • Did not send any captures in over 2 days. • Have sent captures within the past 48 hours. Alternatively, multiply the number of full pages by 20 Devices, then add the number of Devices on the last page.		

*Mark the action as “Not Applicable (N/A) if a checklist item doesn’t apply.

Monitor

Start-of-Year Maintenance Checklist

#	Action	Description	Done*	Notes
1.2	Check if Monitor is monitoring devices	1. Sort the Status column and find devices that have been **offline for over five days** or **haven't sent data in over seven days**. 2. Check the **device name**, **serial number**, and **operating system** for each missing or inactive device.		
1.3	Remove unused devices	• Uninstall Monitor from relevant devices or find unmonitored devices. • In **Monitor** > **Devices**, select the devices, then select **Clear device from list**.		
1.4	Update devices to the latest version of Monitor	Find devices with unsupported Monitor versions and update them to the latest version.		

2. Check Contact Roles

Note: This section is to be completed by a **Safeguarding Contact**, a **Monitor Admin** or a **User Access Admin**.

#	Action	Description	Done*	Notes
2.1	Assign Safeguarding Contact roles	• **Safeguarding Contacts** can assign Contact Roles, receive notifications and calls from Moderators, review all Alerts, and manage Alerting Profiles. • **Limited Safeguarding Contacts** can receive notifications and calls from Moderators and view Alerts for students in their Alerting Profiles.		
2.2	Check Safeguarding and Limited Safeguarding Contacts' details	Check that **Safeguarding** and **Limited Safeguarding Contacts** have the correct email and phone numbers. If needed, update their **names**, **phone numbers**, and contact roles. **Important:** At least **one** contact must have a phone number for emergency calls.		
2.3	Check IT Contacts	Ensure users who need to install Monitor on devices and add or manage other IT Contacts are assigned as **IT Contacts**. Add or edit IT Contacts if needed.		
2.4	Check Reporting Contacts	Ensure users who only need summaries of Monitor activity are assigned as **Reporting Contacts**. Add or edit Reporting Contacts if needed.		

3. Check Admin Roles

Note: This section is to be completed by a **Monitor Admin** or a **User Access Admin**.

#	Action	Description	Done*	Notes
3.1	Check Monitor Admin	In **Monitor > Settings > User Access Management**, assign the Monitor Admin role to the relevant user. Monitor Admins can: • Give Admin roles to other users. • Edit user profiles. • Create and update contacts. • Remove a Monitor product role from a user. **Note:** As part of the migration to the new Monitor version, Safeguarding and IT Contacts were given the Monitor Admin role. You can change who has this role at any time.		
3.2	Check or assign User Access Admin	In **Monitor** > **Settings** > **User Access Admin,** assign the **User Access Management** role. User Access Management: • Works at the account level and can be assigned to any user. • Applies to all products and organisations. • Manage users' contact roles across all licensed products. **Note:** As part of the migration to the new Monitor version, Directory Admins were given the User Access Admin role. You can change who has this role at any time.		

4. Check Alert settings and Alerting Profiles

Note: This section should be completed by a **Safeguarding Contact.**

#	Action	Description	Done*	Notes
4.1	Check Alerts	1. Investigate outstanding Alerts from the past year. 2. Resolve Alerts before the new school year starts.		
4.2	Set up custom Alerting Profiles for certain groups	1. Identify student groups that need different Monitor Alert settings. 2. Ask your Directory Admin to create these groups. 3. Create custom Alerting Profiles for these groups and assign the responsible Safeguarding Contacts.		
4.3	Check Email Alert Levels in Alerting Profiles	Ensure Email Alert Levels appropriately trigger notifications to the Safeguarding and Limited Safeguarding Contacts assigned to the profile.		
4.4	Check the Integration Alert levels in Alerting Profiles	Check that the integration Alert levels are set correctly for logging Monitor Alerts in your connected record-keeping system. See the integration help articles for: • CPOMS (UK) • MyConcern (UK) • CrisisGo (US)		

5. Check directories

Note: This section is to be completed by a **Directory Admin** or a **User Access Admin**.

#	Action	Description	Done*	Notes
5.1	Check synced directories	Check that you have all the Directories you need. Add or delete the Directories, as required.		
5.2	Sync inactive directories	Manually sync Directories with last sync dates older than seven days. • Sync Azure Directory • Sync Google Directory • Sync Windows AD		
5.3	Check User Groups in the Admin Panel	1. Ensure current groups have the required user types for Alerting Profiles. 2. Add new year Groups or new Groups. Your Safeguarding Contact may need to update the Target Groups in their Alerting Profiles.		

6. Check integrations

Note: This section is to be completed by an **Integration Admin**.

#	Action	Description	Done*	Notes
6.1	Check cloud integration	Go to the **Admin Panel** > **Cloud Storage Integration** page and set up the Cloud Scan integration for Microsoft or Google (if included in your licence package).		
6.2	Manage cloud integrations	Edit or turn integrations off or on as needed.		