

School IT incident record template

Record the impact, useful evidence, next action and verified outcome of a school IT fault.

Use this when a fault needs a clear history or will pass to another technician. Start with the effect on the school day, rather than a guessed technical cause.

Reference, time and owner

Use the approved ticket reference, the time the fault was reported and the role responsible for the next action.

Impact and scope

State which rooms, services and tasks are affected, and which checked examples still work.

Observed evidence

Copy the exact error and record relevant timestamps. Link to restricted evidence in the approved system.

Checks and changes

Record each check, its result and any authorised change. Separate observation from interpretation.

Next action and update

Give the next check, its owner and a specific update time. Keep unresolved work open.

Outcome, verification and learning

Record the recovery test, confirmation from the affected user and one practical improvement.

Use approved record references. Keep passwords and sensitive information in their authorised locations.

School IT outage update template

Give school staff a concise service update with known impact, an approved alternative and the next update time.

Use this when several people need the same service information. Keep the technical investigation in its own incident record; the update should help staff decide what to do now.

Service and update time

Name the affected service and give the time of this update.

Known impact

Describe the affected school task, locations and checked scope.

What is known

State confirmed facts and what is still being investigated. Avoid speculative causes.

Approved alternative

Give the alternative agreed with the responsible school lead, or explain who is arranging it.

Owner and next update

Name the accountable role and the next update time, even when a repair estimate is unavailable.

Recovery confirmation

Explain which checks must pass before staff are told the service has recovered.

Use approved record references. Keep passwords and sensitive information in their authorised locations.

School IT new-starter checklist

Coordinate authorised accounts, role access, equipment and a checked handover for a new member of school staff.

Use this after an authorised starter request. Keep names and identity evidence in the school's approved HR and service systems; use the reference here rather than duplicating personal records.

Request and approved start

Record the authorised request reference, role and required start date.

Identity and existing account

Check the authoritative record and whether an account already exists. Record completion, not identity documents.

Role and access approval

Identify the approver for groups, shared resources, licences and school systems.

Managed equipment

Record the approved asset reference, necessary applications and relevant management checks.

User handover

Check the actual sign-in and task, then explain support, security reporting and the agreed account-recovery route.

Exceptions and completion

List missing access with owners and dates. Record who verified the completed handover.

Use approved record references. Keep passwords and sensitive information in their authorised locations.

School IT staff-leaver checklist

Coordinate access removal, assets, work ownership and retention decisions through an authorised staff-leaver process.

Use this with the school's authorised leaver request. Access changes, information retention and any hold must follow the responsible owners' instructions; a checklist cannot decide these for them.

Authority and timing

Record the authorised request and agreed access-change time.

Systems and access owners

List the relevant account, application and physical-access owners using approved references.

Work and retention decisions

Identify the authorised successor, information owner, retention decision and any hold before deletion is considered.

Access and session checks

Confirm the approved account, session, token and delegated-access actions with their owners.

Equipment and physical credentials

Record returned devices, cards and keys against the asset and access registers.

Verification and exceptions

Obtain owner confirmation. Give each remaining action a responsible role and review date.

Use approved record references. Keep passwords and sensitive information in their authorised locations.

School IT technical handover checklist

Make school IT ownership, dependencies, supplier routes and open work understandable to the next person.

Use this before a change of technician, service provider or responsibility. It is an index to approved records, rather than a place to copy passwords or sensitive configuration.

Services and accountable owners

List essential school services, their business owners and technical cover.

Documentation and access route

Give approved document locations and explain how authorised access is requested. Keep secrets in the authorised vault.

Assets and dependencies

Reference the inventory, network overview, relevant contracts and service dependencies.

Backup and recovery evidence

Identify the backup owner, recent status evidence, last recorded restore exercise and unresolved gaps.

Open incidents and upcoming work

List known faults, renewals, exam or termly readiness work, owners and dates.

Acceptance and follow-up

Agree a walkthrough, questions, unresolved risks and the date on which responsibility is accepted.

Use approved record references. Keep passwords and sensitive information in their authorised locations.

Termly school IT readiness checklist

Plan evidence-based checks for teaching spaces, managed devices, service ownership and recovery before a busy school period.

Use this with the school calendar and the owners of each service. Agree the checks and any planned changes early enough to resolve problems before staff and pupils depend on the service.

Period, scope and owners

Record the relevant dates, buildings, services and responsible roles.

Classroom and user-task checks

Test an agreed sample of displays, audio, printing, connectivity and staff sign-in using the intended workflow.

Managed-device readiness

Confirm required applications, management status and planned update or deployment work with device owners.

Operational evidence

Check service contacts, supplier cover, current backup status and the recorded recovery-test position.

Dependencies and contingency

Coordinate events and assessments with their responsible leads. Record the approved alternative for unresolved services.

Readiness decision

List outstanding work with owners, due dates and the role accepting any remaining operational risk.

Use approved record references. Keep passwords and sensitive information in their authorised locations.

Worked example: an incident record

Fictional training data. This is an example of the structure, not a record of a real school incident.

Reference, time and owner

DEMO-104, 08:35. Classroom support technician.

Impact and scope

One teaching-room display reports No signal. The laptop screen works. The next lesson starts at 08:50.

Observed evidence

Display is on HDMI 2; the labelled laptop cable is connected to HDMI 1. No wider outage has been established.

Checks and changes

With the teacher's agreement, selected HDMI 1. No settings on the laptop or network changed.

Next action and update

Technician to verify the lesson display and audio before 08:45.

Outcome, verification and learning

Teacher confirmed the intended slide and audio played. Technician to update the input label and review the classroom quick card this week.

Before closing the record

- Could another technician continue without repeating your checks?
- Does every open action have an owner and update time?
- Does the recorded outcome describe a real verification test?