Incident Management

Incident Management Contents

Key

Glossary term: Glossary term

Cross reference: Cross reference

Becta ICT Advice

Incident Management

Publication date March 2004
Originally published online in September 2003 as part of the Becta website
http://www.becta.org.uk/tsas

Becta
ICT Advice
British Educational Communications
and Technology Agency,
Millburn Hill Road,
Science Park,
Coventry CV4 7JJ

Incident Management

InM 1 Introduction to Incident Management

The computer stops working, you tell someone and you get a replacement computer the same day. Does this sound like your school? If not, you need to introduce the FITS Incident Management process.

InM 1.1

Aim

The aim of this section is to introduce the topic of incident management and to help you implement the process in your school with a minimum of preparation and training.

InM 1.2

Objectives

The objectives of this section are to enable you to:

- understand the difference between incidents and problems
- understand how workarounds and quick fixes can help keep your school computers running
- understand when and when not to commit time and effort on reported faults
- decide whether you can operate a policy of keeping spares for swap outs
- decide whether you need to train your technical and non-technical staff in the Incident Management process
- understand how to produce incident management reports.

InM 2 Overview

InM 2.1

What is Incident Management?

Incident management is a defined process for logging, recording and resolving incidents.

The aim of Incident Management is to restore the service to the customer as quickly as possible, often through a workaround or temporary fixes, rather than through trying to find a permanent solution.

InM 2.1.1

Differences between Incident Management and Problem Management

- The aim of incident management is to restore the service to the customer as quickly as possible, often through a workaround, rather than through trying to find a permanent solution.
- Problem management differs from incident management in that its main goal is the detection of the underlying causes of an incident and the best resolution and prevention.
- In many situations the goals of problem management can be in direct conflict with the goals of incident management.

- Deciding which approach to take requires careful consideration. A sensible approach would be to restore the service as quickly as possible (incident management), but ensuring that all details are recorded. This will enable problem management to continue once a workaround had been implemented.
- Discipline is required, as the idea that the incident is fixed is likely to prevail. However, the incident may well appear again if the resolution to the problem is not found.

InM 2.1.2

Incident vs problem

An incident is where an error occurs: something doesn't work the way it is expected. This is often referred to as:

- a fault
- error
- it doesn't work!
- a problem

but the term used with FITS is 'incident'.

A problem can be:

- the occurrence of the same incident many times
- an incident that affects many users
- the result of network diagnostics revealing that some systems are not operating in the expected way.

Therefore a problem can exist without having immediate impact on the users, whereas incidents are usually more visible and the impact on the user is more immediate.

InM 2.1.3

Examples of incidents

InM 2.1.3.1

User-experienced incidents

Here are some examples of user-experienced incidents. There are three categories: application, hardware and user requests.

1. Application

- Service not available (this could be due to either the network or the application, but at first the user will not be able to determine which)
- Error message when trying to access the application
- Application bug or query preventing the teacher or student from working
- Disk space full
- Technical incident

2. Hardware

- System down
- Printer not printing
- New hardware, such as scanner, printer or digital camera, not working
- Technical incident

3. User requests

- Request for information, advice or documentation
- Forgotten password

- Need to unlock email system
- Training required

InM 2.1.3.2

Technical incidents

Technical incidents can occur without the user being aware of them. There may be a slower response on the network or on individual workstations but, if this is a gradual decline, the user will not notice.

Technicians using diagnostics or proactive monitoring usually spot technical incidents. If a technical incident is not resolved, the impact can affect many users for a long time.

In time, experienced users and the service desk will spot these incidents before the impact affects most users.

Examples of technical incidents

- Disk space nearly full – but this will affect users only when it is completely full.
- Network card intermittent fault – sometimes it appears that the user cannot connect to the network, but on a second attempt the connection works. Replacing the card before it stops working completely provides more benefit to the users.
- Monitor flickering – it is more troublesome in some applications than others. Although the flicker may be easy to live with or ignore, the monitor will not usually last more than a few weeks in this state.

InM 2.2

Why use Incident Management?

There are major benefits to be gained by implementing an incident management process:

- improved information to school leaders on aspects of service quality
- improved information on the reliability of equipment and, ultimately, what people regard as a 'good buy'
- better staff confidence that a process exists to keep their computers working
- greater technician confidence that the users understand what their job involves
- certainty that incidents logged will be addressed and not forgotten
- reduction of the impact of incidents on the school
- resolving the incident first rather than the problem, which will help in keeping a service available (but beware of too many quick fixes that problem management does not ultimately resolve)
- working with knowledge about the configuration and any changes made, which will enable you to identify the cause of incidents quickly
- improved monitoring and ability to interpret the reports, which will help to identify incidents before they have an impact.

InM 2.2.1

What happens if Incident Management is not used?

Failing to implement incident management may result in:

- no one to manage and escalate incidents
- unnecessary severity of incidents and increased likelihood of impact on other areas (for instance, a full disk will prevent printing, saving work and copying files)
- technicians asked to do routine tasks such as clear paper jams; repair a 'broke' monitor that has merely had the power disconnected or fix a disk error when a floppy disk was left in during reboot.

- specialist support staff being subject to constant interruption, making them less effective
- other teachers and support staff being disrupted as people ask their colleagues for advice
- frequent reassessment of incidents from first principles rather than referring to existing solutions such as the knowledge database
- lack of co-ordinated management information
- forgotten, incorrectly handled or badly managed incidents.

InM 2.2.2

Issues with deciding on an incident management process

There will be some who that feel implementing a process called incident management in a school is time consuming and not necessary. Be prepared to overcome:

- absence of visible management or staff commitment, resulting in non-availability of resources for implementation
- lack of clarity about the school's needs
- out-of-date working practices
- poorly defined objectives, goals and responsibilities
- absence of knowledge for resolving incidents
- inadequate staff training
- resistance to change.

InM 2.3

Who uses Incident Management?

Any organisation that needs to understand its technical support requirements should start with implementing a service desk, closely followed by a defined incident management process.

- It will help to channel all incidents through a single point of contact (service desk) so that someone is responsible for following them through to a speedy resolution.
- Most organisations that rely on computers, including schools, need to know how their ICT systems are functioning, what is failing and how long systems are unavailable.
- The reports produced in the process of incident management focus on the performance of equipment, and not on the technical issues that created the incidents.
- The size of the organisation does not matter: Incident Management will enable school leaders and their staff to understand what to do and how to do it.

InM 2.4

How Incident Management works

Incident Management is about understanding the incident life cycle and the actions to take at each stage.

InM 2.4.1

Incident process

InM 2.4.1.1

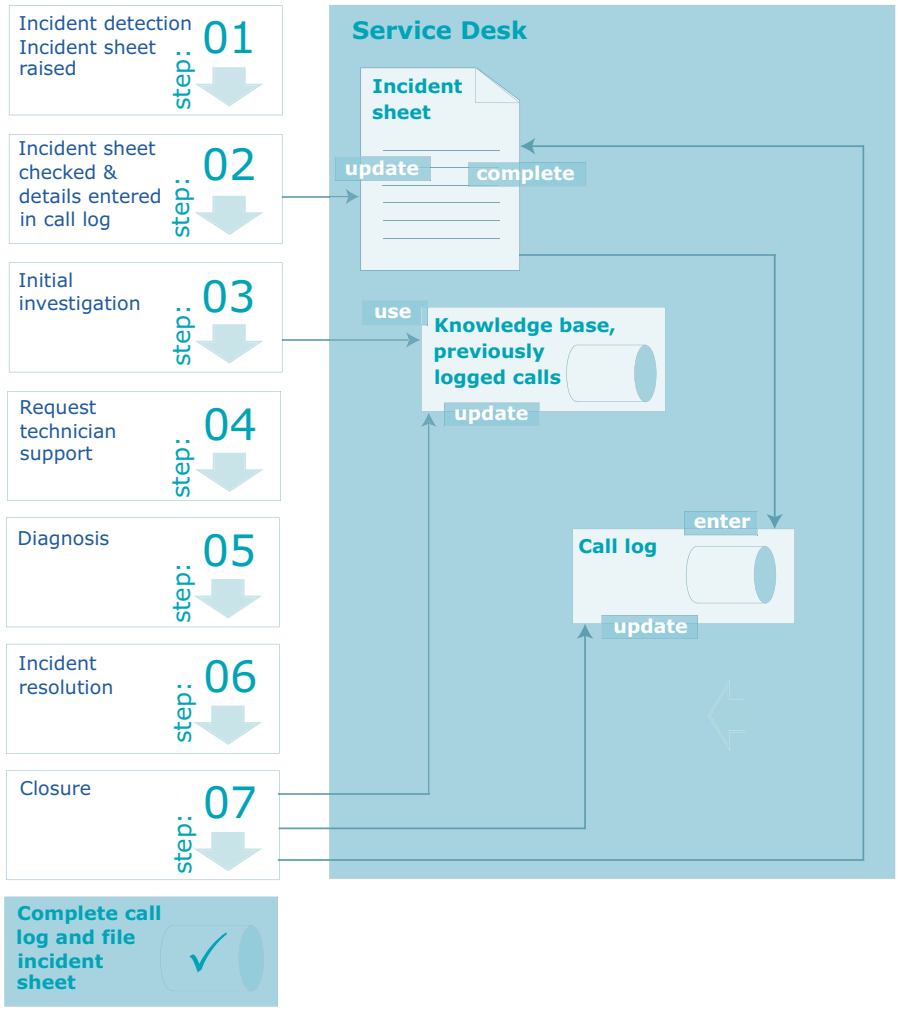
Input to the incident process

These are the usual methods an incident becomes apparent:

- incident details via incident sheet and Service Desk
- configuration details from the configuration management database
- output from problem management and known errors

- resolution details from other incidents
- response to a request for change.

Technicians should complete an incident sheet when they detect a new incident.



Steps in the incident-handling process showing actions by the Service Desk

InM 2.4.1.2

Output from the incident process

- Request for change
- Incident resolution and closure
- Updated incident record and call log
- Methods for workarounds
- Communication with the user
- Management information (reports)
- Input to the Problem Management process

InM 2.4.1.3

Activities of the incident process

- Incident detection and recording
- Initial user support by the single point of contact (service desk)
- Investigation and diagnosis
- Resolution and recovery of service
- Incident closure
- Incident ownership, monitoring, and communication

InM 2.4.1.4

Roles and functions in the incident process

- The service desk should be the single point of contact between all roles in the incident process.
- The service desk should log, monitor and track the progress of the incident.
- Technical support diagnoses and resolves the incident or implements a workaround.
- Technical support progresses unresolved incidents through the problem management process.
- Any additional first-line support groups such as configuration management or change management specialists should be consulted.
- Second-line and third-line support groups, including specialist support groups and external suppliers should be consulted.
- User should keep the service desk informed of any further changes to the state of the affected equipment (sometimes computers start working again when different incidents are resolved).

InM 2.4.2

Steps in the incident life cycle

	Detection
1	A user discovers an incident.
	Completion of incident sheet and call log
2	The user completes the relevant sections of the incident sheet and passes it to the service desk.
3	The person manning the service desk checks that the details of the incident are clear.
4	The service desk then completes their part of the incident sheet and puts a summary of the incident in the call log.
	Initial investigation
5	With experience, the service desk will know if the resolution to the problem can be found in the school's knowledge base or if they should contact a technician. The service desk will check the school's knowledge base for a resolution.
6	If the knowledge base provides a solution, try that before contacting a technician. This is where the system agreed by the school will be followed. Options 1. Someone in the school tries the resolution and a technician is not called. 2. The technician is contacted by the service desk and given the resolution found in the knowledge base.

	Request technical support
7	If a resolution has not been found, the technician will be contacted by the service desk and provided with details from the incident sheet. Again the system agreed by the school will be followed. Options 1. Hand, email, post or fax the sheet to the technician. 2. Speak to the technician in person or by telephone and discuss the incident and action taken so far. 3. Leave the incident sheet for collection by the technician.
	Diagnosis
8	Using an incident diagnostics sheet, the technician runs through a checklist of actions to discover the cause of the incident.
9	Having performed the initial checks, the technician decides whether they can fix the incident at this stage. If not, the problem management process should start.
	Diagnosis
10	Resolving an incident is not the same as fixing a problem. The aim of incident management is to get the system working again as soon as possible. If a fix is not available at this stage, the technician must aim to provide a workaround.
11	When implementing a workaround, the technician may well replace the computer that is exhibiting the errors with a spare. Or the technician may identify existing equipment that can be used temporarily instead of the affected equipment.
12	Once the workaround has been implemented, the problem management process could be invoked to try to understand why the incident occurred and to prevent further occurrences. This may involve further cost, so is not appropriate in all incidents.
	Closure
13	If the incident has been resolved, the technician or service desk updates the incident sheet and call log.
14	The technician or service desk files the incident sheet in chronological order, using the date the incident was reported.
15	If the incident has now become a problem, the call stays open in the call log. The incident sheet and call log are updated to show the action taken. The problem management process then starts.

InM 2.5

What does Incident Management cost?

An incident management process that has been designed to meet the school's needs will be cost effective.

- Knowing that calls will be checked for a quick resolution will benefit the teaching staff, who will not have to wait for a technician to arrive.
- School leaders will be providing a reactive service to implement a proactive approach – keeping the teachers' systems working, so that they can teach.
- Knowing that the aim of incident management is to get the system working and not demonstrate the technician's knowledge will benefit the cynical users.
- Knowing that the school is able to understand its systems and have a fair idea of the incident will benefit those providing technical support.
- Knowing the more common incidents within the school will benefit the budget holder, as they will know which are the ideal spares to purchase.

InM 2.5.1

Expenditure on incident management

Initial expenditure

- Creation and printing of incident diagnostics sheets
- Training of service desk staff and technicians in how to run the process
- Design and creation of management reports

It may be cost effective to purchase some diagnostics or tools. Implementing an incident management process will help evaluate the need for these purchases and avoid buying on a 'whim'.

InM 2.5.2

People to run an incident management process

- Service desk staff – who should be in place before you implement an incident management process
- Technician – implementation of the process should not increase the technician time required

InM 2.5.3

Time for incident management

Eventually a well-run incident management process will save time.

- Incidents are logged and managed so they are not dependent on a particular technician.
- Incidents are resolved using the same approach, so training new technical staff in this approach should always be the same.
- Incidents take less time to resolve once an approach and knowledge base are established.

InM 3 Implementation guide

InM 3.1

Define what needs to be done to implement Incident Management

Before identifying your needs, consider what you want to achieve.

- This is an opportunity to re-evaluate the way you have, to date, approached and fixed incidents.
- Rethink the processes and activities of what currently happens. Do your technical staff always try problem management **before** incident management?
- Understand the difference between incident management and problem management. See InM 2.1 What is Incident Management?
- Technical staff will always try to solve the cause of a problem. Their way of thinking needs to change so that they approach it with incident management **before** problem management.
- Choose which areas to improve and which processes to remove.
- You need to sell the idea to the other staff, so make it appeal to yourself first.

InM 3.1.1

The Incident Management process

The process of reporting and resolving incidents is summarised below.

1. Detecting an incident
2. How to report an incident
3. Initial incident investigation

4. Request technical support
5. Using diagnostics
6. Incident resolution
7. Incident closure

See also InM 2.4.2 Steps in the incident life cycle.

InM 3.1.2 Roles and functions in the incident process

- The service desk should be the single point of contact between all roles in the incident process.
- The service desk should log, monitor and track the progress of the incident.
- Technician support diagnoses and resolves the incident or implements a workaround.
- Technician support progresses unresolved incidents through the Problem Management process.
- Any additional first-line support groups such as configuration management or change management specialists should be consulted.
- Second-line and third-line support groups, including specialist support groups and external suppliers should be consulted.
- User should keep the service desk informed of any further changes to the state of the affected equipment (sometimes computers start working again when different incidents are resolved).

InM 3.1.2.1 Service Desk role in Incident Management

The service desk responsibilities include:

- checking that the user has completed the incident sheet
- actioning the incident sheet
- logging the incident in the call log
- performing the initial incident diagnostics
- requesting technician support when required
- ownership of the call, monitoring and communication
- updating records (call log, incident sheet) with the resolution
- closure of incidents
- filing of incident sheet and incident diagnostics sheets
- progressing any follow-up action (for example following through into problem management).

InM 3.1.2.2 Technical support role in Incident Management

The technician's role in Incident Management must still have the same focus – to aim to restore the service as soon as possible. The technician will keep the service desk informed at all stages.

Technician support to diagnose and resolve the incident or implement a workaround

- Receive details of the incident from the service desk with a completed incident sheet
- Perform diagnostics and use the incident diagnostics sheet to record action taken
- Update the incident sheet and the diagnostics sheet
- Resolve the incident with use of workarounds, if required

Technician support to progress unresolved incidents through the problem management process

- Detect possible problems (before incidents are detected) and action through problem management
- Escalate an incident into problem management after implementing any necessary workarounds first to reduce the time pressure to resolve the problem

Additional first-line support groups such as configuration management or change management specialists to be consulted

- More specialised technician within the school
- Contact with third-party support provider
- Internet-based support groups
- Technician in another school or focus group, Becta online forums and so on

Second- and third-line support groups, including specialist support groups and external suppliers

- Specialist software support groups on, for instance, operating systems or applications
- Specialist hardware support groups including manufacturers of printers or PCs
- Specialist suppliers of, for instance, whiteboards, projectors or digital systems

InM 3.1.2.3

User role in Incident Management

1. A user discovers an incident.
2. If possible, the user tries to repeat the conditions that caused the incident to see if the incident recurs.
3. The user completes the incident sheet and passes it to the service desk.
4. It is important for the user to include information about the incident or request:
    - What did they expect to happen (for example; the printer to print a document)?
    - What exactly did happen (for example, the printer power light was on, but a blank page printed)?
    - What did they check (for example, that there was paper in the printer)?
    - To their knowledge, when did the equipment or software last work?
    - Is the user aware that this equipment or software has had the same problems previously?
    - Is there anything further to add that might help with resolving the incident?

It would help the technician if the user were available to discuss the incident. However, careful completion of the incident sheet should avoid the necessity for this.

The user needs to notify the service desk if the incident appears to 'resolve itself' before a technician's visit.

The user is notified by the service desk when the call is closed and informed of the resolution that was implemented.

InM 3.2 Prepare to implement Incident Management

1. Implement the Service Desk first (see SD 3 Service Desk implementation guide).
    - Decide which forms to use to log incidents and how incident management will interface with the service desk.
2. Decide who will take on the responsibility of incident management.

- You may decide to get a keen competent staff member to help the service desk to handle incidents.
- You may decide to train someone in incident management.
- You may decide to ensure that the technical staff focus on incident management and pass call logging and service desk actions to others.

3. Make sure that management commitment, budget and resource is made available before you consider setting up incident management.
   - Ensure that the proposed solution aligns with your school's strategy and vision.
   - Define clear objectives and deliverables.
   - Involve and consult with the school staff.
   - Sell the benefits to the support staff.
4. Plan your training.
   - Service desk training is the first priority
   - Incident management training is next.
5. Decide what to measure and report.
   - Before making changes, you must understand the levels of service you are currently providing with the current resources available.
   - Produce a report on the numbers of calls currently logged, the time taken to resolve them and the time the equipment is unavailable – this is your baseline.
   - Set targets for a manageable number of objectives for the effectiveness of incident management. Consider this carefully, because after implementation the review will be compared with reality.
   - Decide when to produce your first reports and what to report on. Keep it simple and focus on areas that matter, such as how long a teacher was without a computer resource.

InM 3.2.1

Identify the users of Incident Management

Anyone who comes into contact with using computer equipment, or the results of using it, is potentially a customer of incident management.

This could include:

- teachers
- classroom assistants
- students
- administration staff
- technicians
- headteacher
- technical support staff
- governors.

Also staff involved with cleaning and maintenance could be the first to notice damage, together with those in the school out of school hours:

- caretaker
- cleaners
- students at evening classes
- members of after-school clubs.

InM 3.2.2

Identify who will staff Incident Management

Incident management is a process that can be implemented by anyone following the advice given here. However, the staff mainly involved in carrying out incident management would be:

- the person manning the service desk (the single point of contact)
- competent users at the school
- technicians and other technical support staff.

InM 3.2.3

Plan your training

Prepare a training plan for:

- users on how to use the service desk
- service desk support staff on their role
- staff providing technical support on their interaction with the service desk
- any third-party suppliers on their interaction with the service desk
- school leaders on their interaction with the service desk.

Decide how to deliver the training:

- through notes
- someone showing each person individually
- setting up a training session.

InM 3.2.4

Plan your Incident Management training

It is no coincidence that planning your service desk training comes before incident management. Incident management needs a good support structure if it is to succeed. The service desk provides the support structure.

- Plan which incident management forms you will use.
- Decide which staff will be implementing incident management and following the processes.
- Train the incident management staff on their roles and your expectations.
- Ensure that all technical support staff understand the incident management process.
- Ensure that there are follow-up processes and methods for escalation and that all technical support staff understand.
- Ensure that you know how much time to allocate to solving an incident and at which stage an incident becomes a problem (see Problem Management).
- Decide which spares to keep. Train your staff how to use the spares and get broken equipment fixed or sent away to be fixed.
- Train the staff in tracking progress of calls and how to keep technical staff and users informed.
- Ensure that several staff know how to run incident management so that it continues to work when the usual staff are away.
- Ensure that the training includes how to check the knowledge base and close calls.
- The training should include reasons why the process requires following and what happens if it is not followed.

The Incident Management implementation plan

Implementation plan for introducing Incident Management			
Identifier	**What**	**When**	**Who**
1	Decide who will be your incident management technician.		
2	Decide what training the technician requires.		
3	Decide what training the service desk staff will require.		
4	Arrange and implement the required training.		
5	Decide how the service desk will pass calls to the technician.		
6	Decide what documentation will be used in incident management.		
7	Create or download required incident management forms.		
8	Ensure that the technician and service desk staff know how to use the forms.		
9	Decide whether to use a knowledge base.		
10	Decide on the format of the knowledge base.		
11	Create and populate the knowledge base.		
12	Check whether any workarounds, such as spares, already exist within the school.		
13	Document any workarounds and make them available to the technician.		
14	Document the process for incident management.		
15	Ensure that the technician and service desk staff can understand and follow the incident process.		
16	Test the knowledge base, the functionality of the forms and the usability of the process.		
17	Include any changes to the process identified from testing.		
18	Decide how resolutions will be written up and recorded.		
19	Decide who carries out follow-up actions and how these will be done.		
20	Decide on the review process.		
21	Decide how to keep staff informed.		
22	Plan your first communication to the school about Incident Management.		
23	Decide whether you need to run a pilot of the process.		
25	Carry out the pilot and pilot review.		
26	Include any changes in the system from the pilot review.		
27	Plan the launch date of incident management.		

Implementation plan for introducing a Incident Management			
Identifier	**What**	**When**	**Who**
28	Check that all training has occurred and any changes implemented.		
29	Launch the process of Incident Management.		
30	Carry out the first review and feedback to all.		

For a template of this plan, see Appendix A.

- Have a plan
- Follow the plan
- Have a fallback plan

InM 3.3.1

How to communicate the process to existing users

- Involve your users, and let them know what to expect from the new process.
- Adopt a phased implementation approach.
- Involve/consult your technical support and service desk staff.

The service desk charter would not require altering at this stage as it already includes references to incident management.

InM 3.3.2

What to include in your initial service desk charter

- That diagnostics checklists should be available
- Description of what these are: incidents, requests and problems
- Single point of contact (SPOC) details and responsibilities
- Hours of cover in school
- Hours of cover from a service provider or those providing technical support
- Aims of the service desk

1. To enable incidents and requests to be dealt with quickly and effectively
2. To ensure that an incident only requires reporting once
3. To ensure that those providing technical support understand the details to enable them to resolve incidents as quickly as possible
4. To provide a system that is up and running, even if only a temporary repair, but to ensure it is fixed completely within a specified time
5. To get best value for money from those providing technical support by providing good quality information about incidents and requests
6. To ensure that requests meet the school's internal ICT policy and that purchases are approved through the agreed processes
7. To report on trends, common incidents and their resolution to the staff that find them helpful
8. To support information to school leaders on ICT areas that require more attention or expenditure

InM 3.3.3

Sample document to users about the introduction of Incident Management

Dear …….,

Introduction of Incident Management to our school

We have decided to introduce a new service from the service desk called Incident Management. In order to keep equipment functioning, incident management aims to restore the service as soon as possible. Recurring incidents and long-term errors will be classed as problems and dealt with in a different way.

Incident management will aim to use spares, identify other equipment that meets your immediate need and use 'quick fixes' to get your computer systems up and running quickly. You should soon see improvements in:

- speedier resumption of service
- effective use of existing and spare equipment
- a focus on keeping the service working
- notification of which services are available.

Incident management is part of the service desk function and you will still be able to log calls using the incident sheet.

The start date of the new service is scheduled for xxxxxx. We shall circulate more details nearer the start date.

For a template of this letter, see Appendix B.

InM 3.4 Incident Management post-implementation review

It is the users' perception rather than availability statistics or transaction rates that, in the end, defines whether the service is meeting their needs.

InM 3.4.1

User satisfaction analysis and surveys

Satisfaction surveys are an excellent method of monitoring user perception and expectation and can be used as a powerful marketing tool. However, to ensure success you should address several key points.

- Decide on the scope of the survey.
- Decide on the target audience.
- Clearly define the questions.
- Make the survey easy to complete.
- Conduct the survey regularly.
- Make sure that your users understand the benefits.
- Publish the results.
- Follow through on survey results.
- Translate survey results into actions.

InM 3.4.2

Measurements

- Do not set targets that cannot be measured.
- Ensure that users are aware of what you are doing, and why.
- Establish a baseline before discussing formal service level agreements (SLAs) with customers. (See FITS Service Level Management.)
- Maintain measurements of what is necessary and viable. For instance, if your staff think that they need feedback on response times – then measure them!

InM 3.4.3

Incident Management reports

The aim of reports is to summarise what you already know, and in technical support to reduce the need for technical expertise to understand the information. They are also useful to summarise in non-technical language, to show where improvements could be made. Often the improvements require expenditure, so having reports to back up your suggestions can prove invaluable.

There should already be reports produced by the service desk on the number of incidents logged each week. Expand on the information in those reports to decide whether your new approach to incident management is effective.

- In addition to recording the number of incidents logged each week, compare the numbers to incidents logged prior to implementing Incident Management.
- You should try and show the average length of time taken to resolve incidents before and after implementing Incident Management (so don't forget to record this information prior to implementation).
- Once implementation is complete, compare figures with those of the previous week to see if the incident level and time to resolve incidents have reduced.
- Where possible, show the types of incident reported and aim to have a 'top 10' of calls. You may be surprised at how 'non technical' most of your incidents are. You could then use this information to implement solutions to the top 10 – which could be time well spent.
- Show the percentage of incidents handled within the agreed response time.
- Show the percentage of incidents closed by the service desk without the need for contacting technical support.
- Show the number and percentage of incidents resolved remotely, without the need for a visit.
- Finally, if you implement problem management with incident management, show the number of incidents and problems each week. Over time it will become easier for the service desk to identify the difference between incidents and problems, so persevere with the reports.

See Appendix C for an incident report example and template.

InM 3.5

Incident Management implementation resources

Service desk resources are designed to aid incident management.

InM 3.5.1

Service Desk checklists and handbooks

A useful addition to your support arsenal is the 'user handbook'. This should contain:

- useful hints and tips for incident solving on commonly used applications and equipment
- any preliminary checks or information that may be required before calling the service desk (for instance, the type of service that is not working, equipment identification numbers and error codes).

Importantly, it should tell customers what to expect when they call and what will happen. The provision of a quality service is only achievable when customers and service desk staff work together.

InM 3.5.2

Technician forms

The technician forms are designed to aid technicians in doing their job. It is always useful to record events as they occur so that nothing is left out, as later a seemingly obscure piece of information may be the key to resolving the incident or problem.

- Incident diagnostics sheet (see Appendix D)

InM 3.5.3 Service Desk forms

- Incident/request sheet (see Appendix E)
- User guide to completing the incident/request sheet (see Appendix F)
- Service desk guide to completing the incident/request sheet (see Appendix G)
- Call log (see Appendix H)
- Service desk guide to completing the call log (see Appendix I)

InM 4 Operations guide

It is important to remember that there are many occasions where a technician has been asked to clean the ball in a mouse or clear a paper jam in a printer. Although the solution is not always obvious when an incident is reported, checking previous incidents and their resolution will be an effective way of using your technician and your budget.

InM 4.1 Who carries out Incident Management?

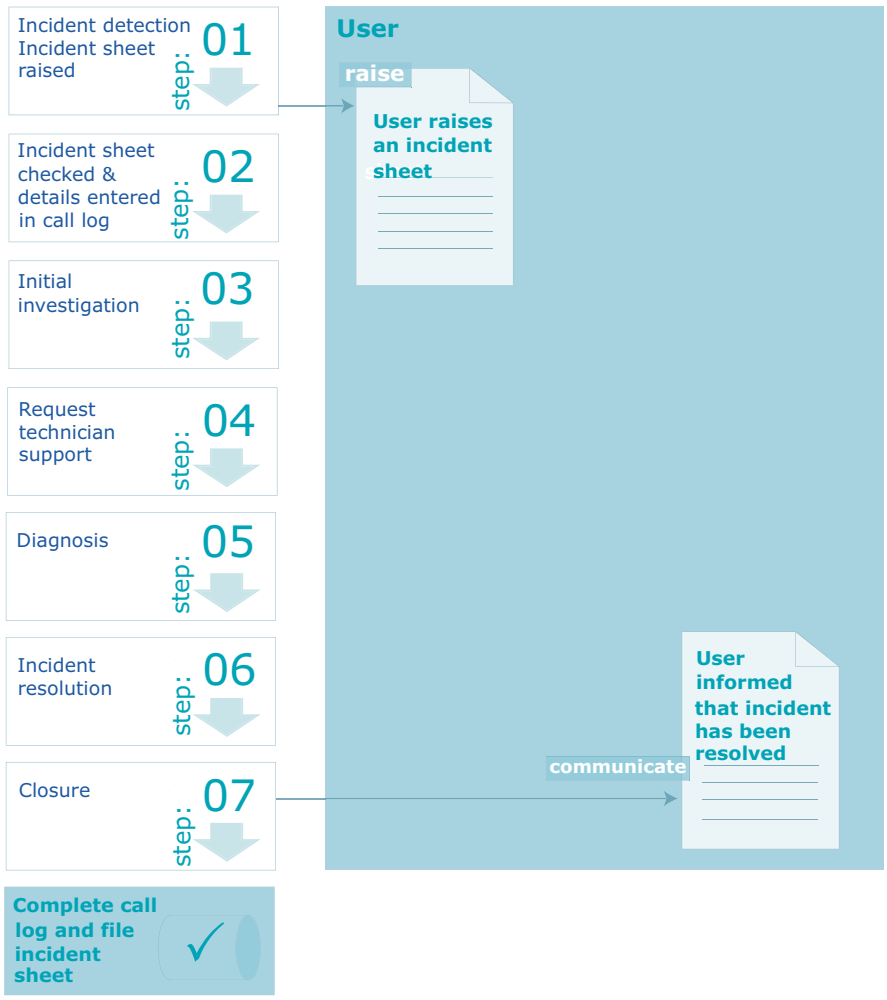
- Incident Management starts with the user discovering the incident and the information they provide on the incident/request sheet.
- The service desk carries out initial investigations into the incident and updates the call log with resolutions.
- A technician or someone providing technical support is responsible for any further incident investigations and for closure of incidents.
- The service desk completes the call log and incident sheet.
- The service desk or technician informs the user of the resolution.

InM 4.2 When does Incident Management occur?

Incident management is run whenever the service desk receives an incident sheet. In a busy school, incident management will form a large part of a technician's typical day.

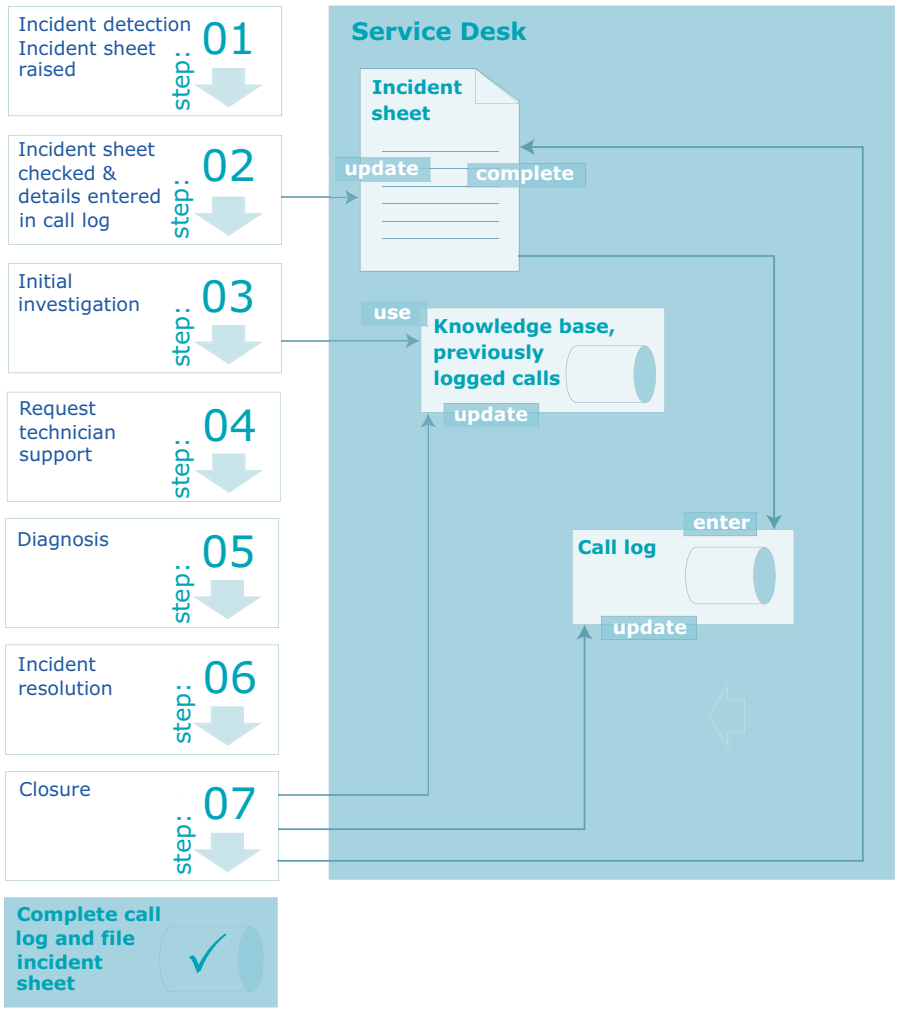
InM 4.2.1 Steps in the incident life cycle

InM 4.2.1.1 Incident life cycle – user



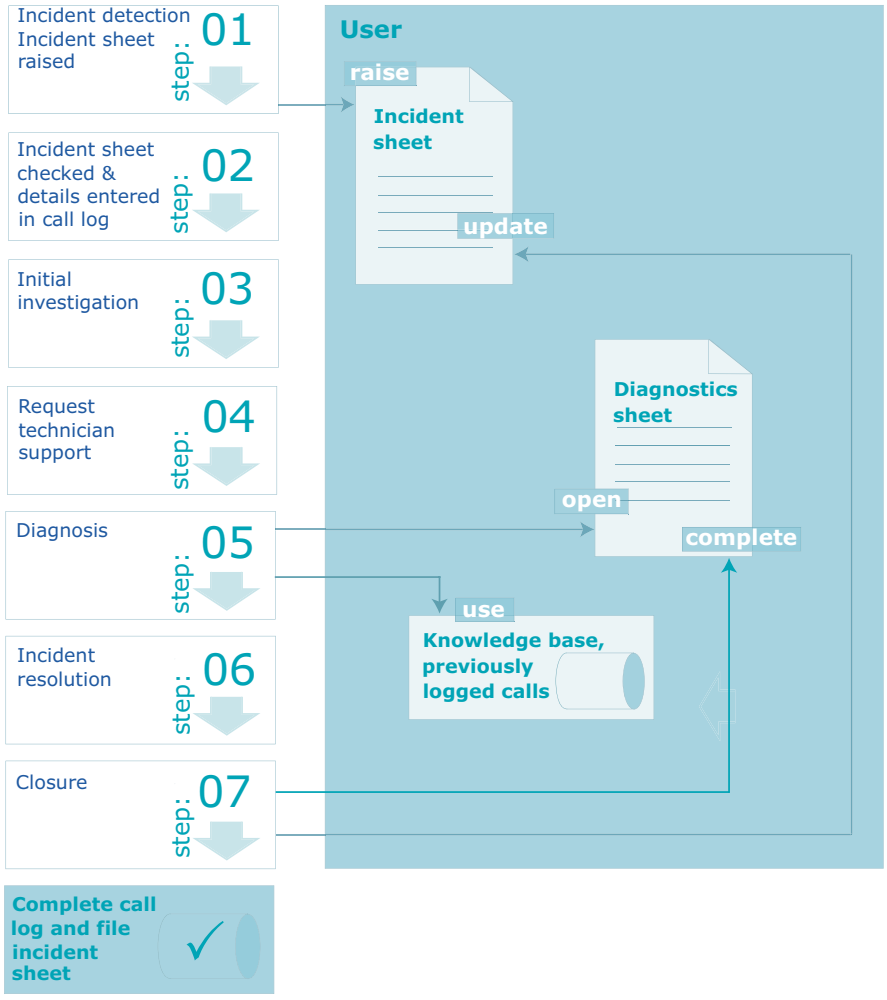
Steps in the incident-handling process relating to the user

Incident life cycle – service desk



Steps in the incident-handling process showing actions by the Service Desk

Incident life cycle – technician



Steps in the incident-handling process showing actions by the technicians

For the incident life cycle explained, see InM 2.4.2.

InM 4.2.2

The Incident Management process

The process in reporting and resolving incidents is summarised below.

1. Detecting an incident
2. How to report an incident
3. Initial incident investigation
4. Request technical support
5. Using diagnostics
6. Incident resolution
7. Incident closure

InM 4.3

How to operate Incident Management

Step 1 Detecting an incident

Incidents are usually detected because an error occurs or the system does not respond as expected. Some of the simplest resolutions find that user expectation is the cause. The system is expected to run some software that has not been installed, or perhaps the user has not followed instructions or has not understood how to operate the system or software because the instructions are not clear.

It is important to discover first whether or not an error really exists. This is where good detection can prevent an unnecessary callout to a technician.

How to detect whether an error has occurred

The user can perform some basic steps to detect whether an error has occurred.

1. Repeat the process that produced the error and see if this occurs again. For example, if you were trying to print, click on the print document icon. This time, take note of what did or did not happen.
2. Try another way to achieve the desired result. Most software will have functions operated by a click on an icon, selecting from a bar menu at the top of the screen or a combination of keystrokes.
3. Look at the screen to see if any error messages are displayed. Windows can often hide the error windows if you have several applications open, so check the bar at the bottom of the screen. Are any of the symbols flashing? If so, click on the symbol to see if an error window has been opened.
4. Write down any error messages on the incident sheet. Also write down which applications were open at the same time. Most importantly, write down when – to your knowledge – this function last worked on this system.
5. If there are no error messages but you succeed in resolving the incident, it may be worth letting your service desk know if the instructions for using the system or software are difficult to understand, don't exist, or need amendment. You could be saving someone else's time with these observations, so use the incident sheet to let the service desk know.

After detection comes the initial incident investigation, usually performed by the Service Desk on receipt of the completed incident sheet.

Step 2 How to report an incident

If you detect an incident, report it. Don't worry if someone else has reported the incident; the service desk will be able to identify duplicate reports.

The impact of not reporting an incident can be great, as unresolved incidents may lead to a lot of disruption. All staff have a responsibility to ensure that others have a good working system, so errors must not be left unresolved. You wouldn't walk past

a fire and hope that someone else raises the alarm: the same approach should follow for computer system incidents and problems.

The incident-reporting process should be simple enough to follow and should not impact on the time or other resources of staff that first detect the error.

Corridor approach

This is a similar way of logging calls as the 'visit office' approach. If a user simply stops a passing technician or person providing technical support to tell them about a fault, they may not even have the opportunity to write down the details of the incident. The user is confident they have 'logged' the incident or request and then feels let down when the call is not acted upon appropriately.

Visit office

The user visits the technical support office to report an incident or make a request. This approach inspires confidence in the user – they have discussed the problem with technical support and know that action will ensue.

If those providing technical support are besieged with visitors and do not have time to prioritise their workload or start working on the incidents, this method does not benefit anyone. The staff providing technical support feel they are very busy, but not prioritising their work reduces their effectiveness. This reactive situation does not embrace best practice.

Paper record of call

The user completes a paper form with details of the incident and posts it in an in-tray used by support staff. The tray is often placed in staff rooms or near reception. Multipart copies are useful in giving users a copy of the details they have logged.

The success of this system relies on technical staff collecting the forms and allocating priorities sufficiently quickly to encourage staff to continue using the system. It will fail if users find their form still in the in-tray later in the day.

Registering details by phone or email

In schools which use external service desks, users may use phone or email to speed up the process of logging calls. The user must be armed with information about the system they are calling about, which may include an allocated asset tag number and machine type.

The speed of response is not determined by the speed with which the call can be logged. Users may become frustrated if they are required to provide lots of information to the support team, only to find that the response is not what they anticipated. It is important to make all users aware of the agreed response times with this service.

Computer interactive

The user uses a simple online form to log the incident or request. The form is easy to follow and is automatically sent to the technical support team. Having completed the form, the user should be confident that the call will be acted upon and will wait for a response from the support team within the published response time.

Because there is no interaction with a person, it is particularly important to respond within the published response time, or users will quickly avoid this method and use the 'corridor' approach instead.

Details to be recorded for service desk calls

- Information about the incident or request
- User impact
- Service desk details (to be completed by the single point of contact)
- Resolution

Benefits and disadvantages of using forms to report incidents

	Benefit	Disadvantage
No technician in school		
When a fault occurs, there is not a technician to tell. In any case, putting the details of the fault in writing removes the ambiguity or brevity that can occur during a conversation.	•	
Clear details of a fault written down can provide time for technicians to prioritise their workload and understand the work involved in solving the fault. This can reduce time and improve efficiency. For example, having full details of the incident may enable resolution through just a quick phone call to the school instead of scheduling a visit.	•	
All faults would need detailed recording to ensure the best possible chance of getting a solution. This is especially important when you do not know who will be dealing with the call.		•
Staff would not be able to get a quick solution, as a technician is not on site. Quick solutions may involve the technician knowing the solution or finding out the solution from a knowledge base – either available in the school or through other sources such as the internet.		•
Technician in school		
When a fault occurs, it is easy for staff to verbally tell the technician the fault details. The staff feel that they have reported the fault and can expect the technician to deal with it. However, the technician may be dealing with another fault and may forget to deal with the new one reported.	•	
Technicians are immediately available to resolve high priority problems and reduce the impact of an incident.	•	
Ambiguity or brevity can occur during a conversation.		•
Just telling a technician in a corridor will not ensure that the work is recorded or prioritised.		•
The technician can feel 'put upon' if stopped in a corridor and asked to do something extra when they are already busy on properly scheduled tasks and this may discourage their efforts to try to prioritise their workload. This will reduce the benefits of their service.		•

Step 3 Initial incident investigation

The service desk staff will check the incident log using key words from the incident sheet. For example, you can search for an error message code in the call log using the find button in the spreadsheet.

With experience, the service desk will know if the resolution to the problem can be found in the school's knowledge base or if they should contact a technician.

If the knowledge base provides a solution, then this should be tried before contacting a technician. This is where the system agreed by the school will be

followed: either someone in the school tries the resolution without calling a technician, or the service desk contacts a technician and gives them the resolution in the knowledge base.

Step 4 Request technical support

If the service desk cannot find a resolution using the knowledge base, they will contact the technician and provide details from the incident sheet. Again, they will follow the system agreed by the school, which may be any of the following:

- email, post or fax the sheet to the technician
- telephone the technician to discuss the incident and any action taken so far
- leave the incident sheet for the technician at their next scheduled visit.

What to do if upgrades are required

In some situations, the resolution to an incident will involve an upgrade to hardware or software. This is where Incident Management links into Release Management and Configuration Management. Upgrades must be planned – even if it involves only one upgrade to one system. If you do not test the upgrade for compatibility with the other software on the system, further errors could occur.

Step 5 Incident diagnosis

The user could perform the first stage of the investigation, if they have the diagnostics tools available and the confidence to proceed. Otherwise it is the school's single point of contact at the service desk who performs the first stage.

In the early days of a service desk, there will be little previous information to check, so the SPOC will pass all calls to the person providing technical support. After about three weeks of operating a service desk, there should be enough information in the call log to enable the SPOC to check previous calls for any similarity.

These checks should be done in the following way:

1. Check the summary of initial action taken and see if a similar incident occurred previously. If a previous incident exists, check details on the incident sheet, which should be filed in date order. If the summary of the incident is the same, where possible try to see if another member of the school's staff can implement the resolution, before calling a technician.
2. Check any diagnostics sheets or diagnostic information supplied to the school to see if there is any help available.
3. Report the incident to the technician.

In all cases, the action taken should be recorded on the incident sheet by ticking or circling the appropriate box.

For more about incident diagnosis, see InM 4.3.1 to InM 4.3.3 below.

Step 6 Incident resolution

The aim of incident resolution is to establish a resolution or workaround as quickly as possible, in order to restore the service to users with minimum disruption to their work.

Incident management at this stage can often be at odds with problem management because:

- incident management aims to get the system back up and running, so a quick fix will do
- problem management seeks to identify the cause of the incident to prevent it being repeated and a quick fix may prevent the problem diagnosis required to identify the cause.

After resolution of the cause of the incident and restoration of the agreed service, the incident is closed.

Step 7 Incident closure

Incident closure is an important aspect of incident management and should not be overlooked.

Once the incident is resolved, closure aims to ensure that the lessons learned are recorded for future use. This is where recording the details of the incident and resolution contribute towards reducing the impact of future incidents.

Category – It is more appropriate at the closure stage to assign a category than when the incident is first reported. Once the incident has been resolved, the knowledge is available about which component or part of the system caused the symptoms of the error.

Known errors – Once an incident has been resolved, the solution becomes a resolution or workaround and can be passed to problem management to be logged as a known error.

Update call log and incident sheet

- Enter the closure details in the call log, including the category of incident (if used by the school).
- Enter the closure details on the incident sheet.
- File the incident sheet in chronological order, using the date when the call was first placed.

InM 4.3.1

Known errors

- A known error is a problem that has previously been successfully diagnosed and for which a workaround has been identified.
- For example, where the cause of the incident is an existing problem with the version of the software, a workaround is a software 'patch' that can be installed. The problem will only be fixed with the next release of the software by the manufacturer.
- A known error can also be referred to as the root cause of a problem (or incident).
- Manufacturers of hardware and software can supply information about known errors.

InM 4.3.1.1

What to do when a manufacturer reports an error condition

Manufacturer notification of error conditions will be circulated through manufacturer websites, suppliers, computer magazines, blanket emails and word of mouth. The outcome of a reported incident may be to find out that it is a known error. Usually known errors of this type have a fix or workaround that can be applied. However, it is frustrating, after reinstalling software, to discover that the error still occurs and has been acknowledged by the manufacturer.

If you know how search engines work, you can look for help with known errors on the internet. Putting the details of any error message or details of the error into a search field may produce several thousand results. Accurate filtering of the results may help you find useful advice on what to do next. With training, experience and confidence, the service desk may be able to use this approach to find known errors before contacting a technician.

InM 4.3.2

Workaround

A workaround is a method of avoiding an incident or problem, either from a temporary fix or from a technique that means the customer is not reliant on a particular aspect of a service that is known to have a problem.

Workarounds are an acceptable way to resolve an incident, since they achieve the aims of incident management: to get the user working again. The service desk or technician must then acknowledge that the underlying problem still needs fixing, but the time taken to achieve this is not having an impact on the user. This leads from a reactive situation into a proactive situation.

InM 4.3.2.1

Workaround examples

1. One of the safest workarounds is to use a different computer or printer where possible until the incident or underlying problem is resolved.
2. If many windows and applications are open on the computer, close them down. Then use the software producing an error on its own to see if the incident recurs. It may be that too many windows were open and the computer does not have enough memory to run lots of applications at once. The workaround is to use one or two applications at a time until more memory can be added to the computer.
3. If the error affects printing, try copying the file to be printed onto a floppy disk or saving it to the file server and then print from another printer. Try to use a printer that has more memory, as printing problems often occur when a complicated file is sent to a printer without much memory. The errors exhibited may not suggest a memory problem, but by successfully printing from a larger-memory printer, you can prove that this was the cause of the incident.
4. Make available to users a list of memory-hungry applications. This will help them decide which applications to shut down first if the computer appears slow or unresponsive.
5. Make sure everyone knows the rules for password resets or email resets. One school has decided to make the password rename to 'diarrhoea', to encourage users to remember their original passwords more often!

InM 4.3.2.2

Spare equipment

Think about the following to see if this could be an effective workaround in your school.

1. Ensure that there are four spare computers. They must really be spare!
2. Configure two of the computers with the school's computer image (standard build – see Release Management F070101 for further information) ready to swap out when required.
3. When an incident occurs that you cannot resolve in 15 minutes, replace the affected computer with one of the spares.
4. Bring the faulty computer back to the technician area.

Do not try to fix the problem.

5. Re-image the faulty computer with the school's computer image.
6. Run a set of pre-approved diagnostic tests on the re-imaged computer.
7. Make the re-imaged computer one of your two spares.

With the other two computers, configure one with any new software and create the new image. Then test the new image on the second computer.

These four computers are not equipment for use in the school as ordinary equipment. If you need to allocate one as an additional resource, ensure that a replacement is ordered and put back into the group of four.

The cost of these four computers compared to lost teaching time, hours of technician time each week, unresolved incidents and problems should pay for the cost of them over and over again. But you must stick to the rules and re-image. Do not try to resolve the incident or problem. This may be boring – but it can be very effective.

InM 4.3.3

How to diagnose incidents

It is possible to own a library of books about IT and ICT and never come across the concept of incidents or errors, except in software programming! It is not an easy subject to describe or on which to produce a guide to the best approach.

Once an incident is reported and passed to a technician to resolve, you then move into the real science of technical support. Sometimes this can appear to the user or customer as a 'black art' – the area where the person with the technical knowledge has a real grasp of the subject and no one else can expect to achieve a result. However, this is not true. Users can do most of the diagnostics themselves and provide a pointer towards where the root cause of the incident really lies. This can help in the speed of resolution and increases the productivity of the technician.

Here is one approach to incident diagnosis that technicians may like to try.

There are several steps but one of the most important is the pause. The pause is the step where you decide which action to take first. If action is taken before the diagnostics, it often becomes more difficult to resolve the incident.

InM 4.3.3.1

Steps in incident diagnosis

Use the incident diagnostics sheet.

1. Establish current status by deciding which area is the likely cause:
   - hardware
   - software
   - network
   - user guide
   - other.
2. Pause and decide which action or actions to take. It is important not to act rashly as this could create further incidents!
3. Take action and record the results. This could be an iterative process, but it is vitally important to record what was done.

There are many examples of what should have been a five-minute fix taking several hours because the technician failed to record the actions taken.

InM 4.3.3.2

Checking the knowledge base

In the early days of incident management, it is likely that the first checks will be in the call log using a keyword search. When the call log grows larger or the decision is made to use databases, it is important to have a search facility. The school should decide which words or types of word should be recorded in the incident resolution. This will enable searches of the knowledge base to be made using those words.

Mature systems may implement the use of categories to help with quick searches of the knowledge base. However, the incorrect use of categories can reduce the effectiveness of searching and the overall usefulness of the knowledge base.

InM 4.3.3.3

Technician diagnostics

The technician does not require an arsenal of diagnostics tools for incidents. More in-depth analysis is done as part of problem management.

See Appendix D for the incident diagnostics sheet.

InM 4.3.3.4

User diagnostics

You can find self-service tools in IinM 4.5.2.1 and the incident diagnostics sheet at Appendix D.

InM 4.3.4

Incident handling

The process for handling incidents from detection through to closure is shown in the diagram below.

Steps in the incident-handling process life cycle

InM 4.4

Measuring the results of Incident Management

See InM3.4 in the Incident Management Implementation guide.

InM 4.5

Incident Management resources

InM 4.5.1

Incident Management checklists

InM 4.5.1.1

Incident detection checklist

- Do you encourage users to repeat the actions that first showed an error?
- Do users know how to check the hardware they are using for loose cables?
- Can users check whether power is supplied to the equipment and turned on?
- Do users know how to check that the start-up screens are running when the computer is turned on?

- Do users know how to print a test page from the printer menus?
- Have the users been instructed how to check if the network cable is attached at both ends?
- Have the school's common error conditions been notified to users, so that they can check these conditions first? For example, can they check whether the power to the monitor has been disconnected?

InM 4.5.1.2

Incident logging checklist

- Are the incidents tracked?
- Has the date the incident occurred been input?
- Has the date the incident was resolved been input?
- Are follow up dates input (where needed) whilst the incident is open?
- Are comments added, to aid with understanding why follow-ups are required?
- Does someone own the incident?

InM 4.5.1.3

Incident investigation checklist

- Is a consistent approach applied to all incidents?
- Is someone taking ownership for this incident?
- Can the call log be checked for previous incidents exhibiting similar symptoms?
- Does a knowledge base exist?
- Do the instructions for using the knowledge base aid in initial investigation?
- Is there a link to the configuration management database to check recent changes made?

InM 4.5.1.4

Incident diagnosis checklist

- Are meaningful records of incidents kept?
- Is a list kept of who is best qualified to diagnose and resolve faults when they occur?
- Is there a list of known errors that can be referred to?
- Is there a list of known workarounds that can be referred to?
- Is there a process to move from incident management to problem management?
- Does the technician complete incident diagnostics sheets?

InM 4.5.1.5

Incident resolution checklist

- Can faults be resolved quickly?
- Is there a communications link between the user and the resolver?
- Is there a process to add new solutions to the known workarounds list?
- Does the technician update the incident sheet from details on the diagnostics sheet?

InM 4.5.1.6

Incident closure checklist

- Are the incident sheets and incident diagnostics sheets filed together?
- Can old incidents be referred to when a similar problem occurs – in other words, is there a knowledge base, even if it is just a basic filing system?
- Is there a link between the call log and the configuration management database to record any changes made?

InM 4.5.1.7

Known errors checklist

- Does the school keep a list of known errors?
- Are there particular errors common to the school such as students removing mouse balls or even hard drives?
- Is the known errors list updated from closed calls?
- Is the known errors list updated from manufacturers' information?
- Does the school share a known errors database with other schools?
- Do the known errors get removed when software upgrades fix the known errors?
- Can school staff interrogate the internet (or school intranet) for known errors and if so is this documented and easy to understand?

InM 4.5.1.8

Workarounds checklist

- Does the school keep a list of workarounds?
- Do the workarounds get implemented to ensure that the user is working quickly?
- Do the workarounds get updated and checked regularly?
- Is there enough spare equipment to enable some of the workarounds to function?
- Has the school enough software licences to implement some of the workarounds (for example, to enable the software to be installed on an additional computer)
- Is the equipment in the school compatible to enable workarounds to be effective?

InM 4.5.2

Incident Management tools

InM 4.5.2.1

Self-service tools

InM 4.5.2.1.1

What are self-service tools?

Self-service tools can offer users a strategy for 'DIY' support, which means they do not always need to rely on direct intervention from technical support.

It is important to identify who will use the tool and what the tool is to be used for.

The tools can be:

- written lists of things to check
- flow diagrams with easy-to-follow instructions
- tools on a CD or on the school network, created by the school technical staff or provider
- online tools through the internet, or downloaded to the school intranet (if it has one)
- diagnostics supplied by the hardware manufacturer or software manufacturer
- telephone support.

InM 4.5.2.1.2

How can self-service tools be used?

How self-service is implemented can vary significantly, depending upon what the school wants to achieve and the range of services being offered.

- Users register their own requests for help with external support suppliers and check on their progress.
- Users then have direct access to support information and knowledge.
- Users are able to manage support requests themselves.

- Users can search knowledge bases for solutions.
- Users can download program updates or bug fixes.
- Users can order goods or services.
- Ease of access and speed of resolution is increased.
- Demand on support resources is reduced.

InM 4.5.2.1.3

A strategy for deploying self-service tools

A successful self-service strategy depends on several important factors: the commitment of the school leadership, properly maintained support processes and good-quality content for the self-service system.

School leadership commitment

- Any initiative that entails change in a school requires leadership support and commitment to execute the initiative.
- See the Change Management process on how to introduce any changes in ICT to your school.
- It is essential to put the right processes and tools in place to ensure that, while the user is in control, they are following a path that is carefully designed by the school or provider.
- Users need to know what self-service channels are in place, along with the value and responsibilities of using them.
- If the decision has been taken to supplement technical support with a self-help tool, users must understand that if the system is unavailable, they should wait and try again and not pick up the phone.
- Email contact should be used, together with online communities, to share the information obtained, where possible.

Support processes maintained

- It is important not to bypass or invalidate any of the existing Change Management and Release Management processes.
- Always complete the incident form, even if the self-service tools enable the incident to be resolved, as time and effort were still spent on the incident.
- You can monitor the effectiveness of the service by measuring what self-help services are being requested, how often and what for.
- Feedback will be required on how effective the suggestions were on resolution, how well they were presented, and whether or not the incident recurred.

Content of the self-service system

- Any system that is not easy to use or that does not contain high-quality content will fail.
- If the users are unable to get the information they need when they need it, they will immediately pick up the telephone next time they encounter a problem.
- If the system does not work well, the support team will find itself supporting yet another application – the self-service system itself.

InM 4.5.2.1.4

To buy or create a self-service system

Buy into a provided self-service system

- Does the system provide benefit to your school?
- Is it cost effective to use a self-service system because of the consequent reduction in staff costs?

- Can you be sure the advice is current and accurate?
- Can you carry out the instructions given by the self-service method?

Create your own self-service system

- Do you have the resource, both now and in the future, to plan, implement, upgrade and maintain your own self-service system?
- Who will support your own self-service system?
- How long will it take to develop?
- Who is going to pay for it?
- When will it be ready?
- What if your 'experts' leave?

InM 4.5.2.2 Incident diagnostics

See Appendix D for the incident diagnostics sheet.

InM 5 Review of Incident Management

The purpose of this section is to help you review your implementation and ongoing operation of incident management, check your understanding of the process, examine what a successful implementation should look like and consider what you have achieved by introducing it into your school. This will help you to assess how successful its introduction has been and point you back to the relevant sections in the Incident Management process that you should revisit to make improvements, if these are necessary.

Start by reading the sections included in the recap of Incident Management. When you have refreshed your memory and considered your own implementation alongside these descriptions, work through the checklist to identify any areas you should revisit and perhaps re-implement or reinforce.

InM 5.1 Recap of Incident Management

Incident management is described in the overview, with the differences between incidents and problems explained. There is an implementation guide providing step-by-step instructions on planning and introducing incident management. The operations guide shows the stages of incident management with the respective work done by the single point of contact and the technician. We also set out the roles and responsibilities of those involved in the process and, in the appendices, provide a number of resources for you to use.

Check your understanding of the process by following InM 5.1.1 to InM 5.1.4 below.

InM 5.1.1 Incident Management summary

Step	Tasks
Define what needs to be done.	• Understand the stages in the incident lifecycle. • Understand the difference between incidents and problems. • Decide which diagnostic processes the school will use. • Decide how to record incidents and requests. • Decide how to provide training and feedback.

Step	Tasks
Prepare to implement.	• Identify the users of incident management. • Identify who will staff the incident management process. • Plan your training. • Plan the forms and documentation you will use. • Get the school leaders to commit to the process.
Implement incident management.	• Follow the implementation plan. • Produce a letter to users. • Include updates to the service desk charter.
Incident management resources	• Incident/request sheet • Incident diagnostics sheet • Call log • Instructions on the use of the forms • Knowledge base • Use of the internet to explain error messages
Post-implementation review	• Workload monitoring • Analysis, surveys and measurements • Incident reports

InM 5.1.2

What you should expect now that you have implemented Incident Management

- You have a process for logging calls with a single point of contact.
- The school has a service desk function.
- All users should be familiar with the method for logging incidents.
- The technicians should understand that they receive calls from the service desk and not the users.
- All staff should understand the need for logging calls through the service desk and should refrain from logging calls directly with the technician.

InM 5.1.3

What you should have achieved through Incident Management

- A standard way of recording and logging incidents and requests
- A method of communication between the user and technician via the service desk
- Historical information about calls to individual equipment
- Historical information about failure rates of equipment
- Reports and feedback on the calls logged and resolved
- Knowledge of the time taken to resolve incidents and requests
- Information about the amount of technician time required to resolve all requests
- A consistent approach to handling calls and how the response to the calls is planned
- Information about the number of calls currently outstanding and how long they have been logged

InM 5.1.3

Benefits of having implemented Incident Management

- Someone manages and escalates incidents.
- You deal with incidents quickly, before they become severe.
- Your technicians deal with incidents rather than just clearing paper jams or changing toner.
- Technicians have prioritised workloads.
- Specialist support staff are able to concentrate on the work that needs their skills.
- Technically able teachers or ICT co-ordinators are left to do their work and are not interrupted to resolve 'errors'.
- You can diagnose incidents quickly, using previous knowledge rather than treating each event as a new one.
- You have co-ordinated management information.
- You can check that suppliers and staff are meeting agreed service levels.

InM 5.2

Checklist

Use this checklist to identify any areas of incident management that have not yet been entirely successful. Then reinforce them by revisiting and re-implementing the relevant section of the FITS process.

Characteristics of a successful implementation	FITS section to revisit if the implementation is not yet successful	
The process for logging an incident or making a request is understood.	Appendix F	User guide to completing the incident/request sheet
The incident sheet is checked for completeness.	Appendix G	Service desk guide to completing the incident/request sheet
The incident sheet is available.	Appendix E	Incident/request sheet
The incident diagnostic sheet and process is understood and used	InM 4.3	How to operate Incident Management Step 5
The school uses a knowledge base.	InM 4.3.3.2	Checking the knowledge base
The service desk advises on the closure of a call.	InM 4.3	How to operate Incident Management Step 7
The levels of reported incidents are monitored and results of the measurements are reported.	InM 3.4.2	Incident Management post-implementation review
The benefits of using Incident Management are realised and there is continuous improvement	InM 4.5.1	Incident Management checklists

If the above characteristics are all true of your school, congratulations on implementing a successful incident management process! The next steps for you are to continue operating the process as described in the Incident Management Operations guide (InM 4) and establish the process firmly. Work through this checklist at regular intervals to help you check that everyone responsible continues to carry out all aspects of the process. You can then refer to the relevant sections above to address any shortfalls as they arise.

Appendices

InM Appendix A Incident Management implementation plan

Implementation plan for introducing Incident Management			
Identifier	**What**	**When**	**Who**
1	Decide who will be your incident management technician.		
2	Decide what training the technician requires.		
3	Decide what training the service desk staff will require.		
4	Arrange and implement the required training.		
5	Decide how the service desk will pass calls to the technician.		
6	Decide what documentation will be used in incident management.		
7	Create or download required incident management forms.		
8	Ensure that the technician and service desk staff know how to use the forms.		
9	Decide whether to use a knowledge base.		
10	Decide on the format of the knowledge base.		
11	Create and populate the knowledge base.		
12	Check whether any workarounds, such as spares, already exist within the school.		
13	Document any workarounds and make them available to the technician.		
14	Document the process for incident management.		
15	Ensure that the technician and service desk staff can understand and follow the incident process.		
16	Test the knowledge base, the functionality of the forms and the usability of the process.		
17	Include any changes to the process identified from testing.		
18	Decide how resolutions will be written up and recorded.		
19	Decide who carries out follow-up actions and how these will be done.		
20	Decide on the review process.		
21	Decide how to keep staff informed.		
22	Plan your first communication to the school about Incident Management.		
23	Decide whether you need to run a pilot of the process.		
25	Carry out the pilot and pilot review.		
26	Include any changes in the system from the pilot review.		
27	Plan the launch date of incident management.		

Implementation plan for introducing a Incident Management			
Identifier	**What**	**When**	**Who**
28	Check that all training has occurred and any changes implemented.		
29	Launch the process of Incident Management.		
30	Carry out the first review and feedback to all.		

- Have a plan
- Follow the plan
- Have a fallback plan

You can download the template from the FITS website
http://www.becta.org.uk/tsas/index.cfm?refsect=ntss&bcsect=default&sect=incident&id=dw1100

InM Appendix B Sample document to users about the introduction of Incident Management

Dear ,

Introduction of Incident Management to our school

We have decided to introduce a new service from the service desk called Incident Management. In order to keep equipment functioning, incident management aims to restore the service as soon as possible. Recurring incidents and long-term errors will be classed as problems and dealt with in a different way.

Incident management will aim to use spares, identify other equipment that meets your immediate need and use 'quick fixes' to get your computer systems up and running quickly. You should soon see improvements in:

- speedier resumption of service
- effective use of existing and spare equipment
- a focus on keeping the service working
- notification of which services are available.

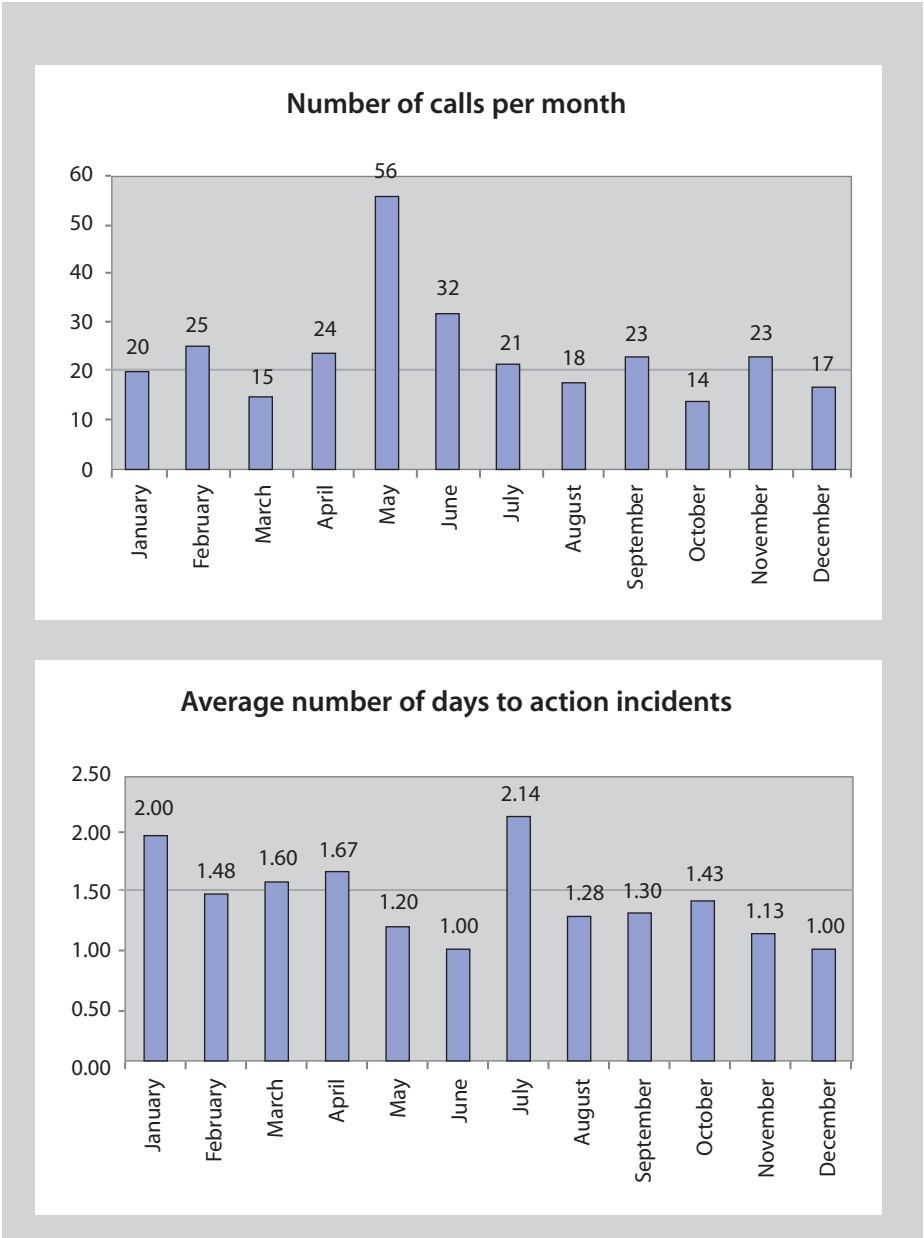
Incident management is part of the service desk function and you will still be able to log calls using the incident sheet.

The start date of the new service is scheduled for xxxxxx. We shall circulate more details nearer the start date.

You can download the template from the FITS website
http://www.becta.org.uk/tsas/index.cfm?refsect=ntss&bcsect=default&sect=incident&id=dw1100&pid=dw1099

Framework for ICT Technical Support (FITS) **Becta | ICT Advice**

Incident report



http://www.becta.org.uk/techicalsupport/
published September 2003

You can download the template from the FITS website
http://www.becta.org.uk/tsas/docs/im_report.xls

Becta ICT Advice

Technical Support Advisory Service (TSAS)
Incident Management

Incident Diagnostics Sheet

Use this form as a guide, but do not leave out detail. Continue on further sheets if necessary

Equipment Unique ID	Name of person	Date & Time of - Incident / Request
Establish current status		
What was expected to happen?		
What did happen? Can the incident be recreated?		
When did it last work? Has it EVER worked?		
What has been changed recently?		
Write down any error messages displayed.		
Can you or anyone else perform the same task on other equipment?		
Which area is the likely cause?		
From the answers above is the problem likely to be hardware, software, network, user guide, other (details please).		

Actions to take

Hardware *Check the knowledge base and fact sheets*	
Which area of hardware is affected?	
Which part requires replacing?	
Which spare equipment is available?	
Install spare or order replacement or other, (please detail).	
Software *Check the knowledge base and fact sheets*	
Which application or operating system is in error?	
Result of checking the error message through tools (eg, the internet).	
Does software require reinstallation or a patch? Please give reasons.	

http://www.becta.org.uk/techicalsupport/
published September 2003

You can download the template from the FITS website
http://www.becta.org.uk/tsas/index.cfm?refsect=ntss&bcsect=default&sect=incident&id=dw1127

Results of reinstallation or patch applied.	
Network ***Check the knowledge base and fact sheets***	
Does the network error affect one or many computers?	
Can the area affected be identified or isolated using diagnostics?	
Which replacement equipment can be installed?	
Actions to take.	
Results of actions taken.	
User Guide ***Check the knowledge base and fact sheets***	
Which user guide is in error, does a user guide exist?	
Can the error be corrected with training or documentation?	
Actions to take.	
Results of actions taken.	
Other ***Check the knowledge base and fact sheets***	
What was the cause of the incident?	
What actions have been taken?	
Which further actions are required?	
Incident outcome	
Has the incident been resolved?	[_] Yes [_] No
What was the final outcome?	
Date and resolver's name.	

Has the incident sheet and call log been updated?	**Has the user been informed?**
[_] Yes [_] No	[_] Yes [_] No

http://www.becta.org.uk/techicalsupport/
published September 2003

You can download the template from the FITS website **http://www.becta.org.uk/tsas/index.cfm?refsect=ntss&bcsect=default&sect=incident&id=dw1127**

Becta ICT Advice

Technical Support Advisory Service (TSAS)

Service Desk / Incident Management

Incident/request sheet

User to complete

Equipment Unique ID	Name of person	Date & Time of Incident or request
Details of incident or request – continue overleaf if necessary		
Equipment required for use by	**Suggested alternative equipment (date and time)**	**Alternative equipment set up by (date and time)**

Service desk to complete

Number of users affected (please circle)				System usage in hours per week (please circle)	
1, 2-5, 6-10, 11-30, 30+				1, 2-10, 11-20, 20+	
Self service available to user	**Check incident log**	**Check user knowledge base**	**Check school knowledge base**	**Check details on internet**	
Y/N	Y/N	Y/N	Y/N	Y/N	
Technician required	**Technician or 3rd party contacted – date and time**		**date and time of response**		
Y/N					
Incident to be resolved at next scheduled visit	**Date of next scheduled visit**	**Does incident require Change Management**	**Follow-up date**		
Y/N	Y/N	Y/N	Y/N		
User notified of action	**Notification given (date and time)**	**Incident/request owner**	**Technical support provided by**		
Y/N	Y/N	Y/N	Y/N		
Incident resolver		**Equipment that caused the incident**			
How was the incident resolved? (Add further pages as necessary)					
Further action required					
Was equipment removed, installed or swapped as a result of this incident/request?		**Configuration-management database updated**			
Y/N		Y/N			

http://www.becta.org.uk/techicalsupport/
published September 2003

You can download the template from the FITS website **http://www.becta.org.uk/tsas/index.cfm?refsect=ntss&bcsect=default&sect=servdesk&id=dw1039**

Becta ICT Advice

Technical Support Advisory Service (TSAS)
Service Desk / Incident Management

User guide to completing the incident request form

1. Equipment unique ID

If this is not available, describe where the equipment is located. Don't forget to leave a note on faulty equipment to show that you have reported an incident.

2. Information about the incident or request

What did you expect to happen? (eg, the printer to print a document)

What exactly did happen? (eg, the printer power light was on, but a blank page printed)

What did you check? (eg, that there was paper in the printer)

When, to your knowledge, did the equipment or software last work?

Has this equipment or software had the same problems previously that you know of?

Do you have anything further to add that might help with resolving the incident?

3. Equipment required for use by

When do you next expect to use this equipment?

4. Suggested alternative equipment (and date it will be required)

If you know which other equipment would serve the same purpose, it is helpful to the service desk to know in advance to enable it to be set up.

Note

The rest of the form will be completed by the service desk and those providing technical support.

Please ensure that the form is passed to the service desk quickly for action.

http://www.becta.org.uk/techicalsupport/
published September 2003

Becta ICT Advice

Technical Support Advisory Service (TSAS)
Service Desk / Incident Management

Service Desk guide to completing the incident/request form

Check that the part for the user to complete is filled in.

- Equipment's unique ID – check that this has been completed (it is mandatory).
- Information about the incident or request – does it make sense?
- Equipment required for use by – this should be completed.
- Suggested alternative equipment (and date required) – action if you are able to arrange access to the requested alternative equipment (before attending to the faulty equipment).
- At this stage you should have enough information to start an entry in the call log. See the Service Desk guide to completing the call log.

Action by service desk

- Alternative equipment set up – complete the date and time when this has been actioned or write 'N/A' if not required.
- Number of users affected – circle the appropriate number. This is to help the technician but, if you don't know, write 'unsure' in the box.
- System usage in hours per week – circle the appropriate number. This is to help the technician but, if you don't know, write 'unsure' in the box.
- There may be sources of help available to the user without calling out a technician. If any of these have been used, please indicate by circling 'Y'; otherwise circle 'N'.
- Indicate whether a technician is required, as the problem may have been solved before a callout is required.
- Put the date and time the technician service was contacted. This is important, as it may be used to measure the reliability of service levels.
- Put the date and time the technician service responded. Again, this may be required to help with service-level reliability.
- Complete the boxes for the technician's next visit and change management, as this form is for logging incidents or requests.
- As it is important to keep the user notified, ensure that the details of when the user was notified are recorded on the form.
- Technical support provided by – this is the technician's name if a technician is used.
- Incident resolver – this should always be completed, even if the incident cannot be resolved. This identifies the person making the decision about the outcome of the call.
- Equipment that caused the incident – this will help identify solutions to incidents in the future.
- How the incident was resolved – a summary provided by the person resolving the incident. More detail can be provided on continuation sheets.
- Further action required – does additional software require installing? Is a fix ready for the future? Does equipment require ordering?
- Was equipment moved, installed or swapped? – circle 'Y' or 'N'.
- Was the configuration-management database updated? – circle 'Y' or 'N'.

Once the incident/request form is complete, enter the details into the call log.

http://www.becta.org.uk/techicalsupport/
published September 2003

Becta | ICT advice

Framework for ICT Technical Support (FITS)

Service Desk / Incident Management call log

Call no	Date of call	Time of call	Equipment unique ID	Name of person	Incident or problem	Summary of initial action taken	Date action expected	Date action occurred	Resolution - fixed/not fixed/no action/follow up	Further action required	Summary of incident	Date closed

http://www.becta.org.uk/techicalsupport/
published September 2003

im_call_log_xls
page 1 of 2

You can download the template from the FITS website
http://www.becta.org.uk/tsas/index.cfm?refsect=ntss&bcsect=default&sect=servdesk&id=dw1040

Becta ICT Advice

Technical Support Advisory Service (TSAS)
Service Desk / Incident Management

Service Desk guide to completing the call log

1. Call number – if you wish to use a numbering system, allocate the next number in sequence. You may put this number onto the incident/request sheet. However, calls can usually be referenced using the date and unique ID.

2. Date of call –use the same date format for all date entries, especially if you keep the call log as a spreadsheet.

3. Time of call – again use a consistent time format, as this will enable accurate reports to be produced.

4. Equipment unique ID – if this is not available, describe where the equipment is located. Check whether a note has been left on faulty equipment to show that the incident has been reported.

5. Name of person - if you only put first names, ensure that your process can distinguish between people.

6. Summary of initial action

- Call fixed by caller
- Self-help website used - and if it did or did not work
- Where previous log was checked, if this resolved the incident
- Whether knowledge base checked, and if this did or did not work
- Whether technician required or not
- Show whether this is a request or an incident

7. Date action expected – when is the technician expected to work on the incident?

8. Date action occurred – if you don't use this, you will not be able to check whether your technician or technical support provider is conforming to the agreements in place.

9. Resolution – don't put in here what was done – that goes in the summary. Do put in the status – fixed, not fixed, replacement required, follow up required, etc.

10.Further action required – you can leave this as a separate entry if you always have a lot of follow-up action, or it can be combined with the resolution field.

11. Summary of incident – as you will probably use the information on the incident/request sheet when logging a call with a technician, don't be tempted to complete the summary of incident until after the resolution. This enables the call log to be used as a reference for similar incidents.

The call log has been designed to print as 1 page (landscape) for easy reading. Adjust it to meet your needs and realise that it may take several revisions before you arrive at the format that works for you. Change it as often as necessary until you get it right.

http://www.becta.org.uk/techicalsupport/
published September 2003

Glossary

10Base-T	A networking standard that supports data transfer rates up to 100 Mbps (100 megabits per second). 10Base-T is based on the older Ethernet standard but is 10 times faster than Ethernet; it is often referred to as Fast Ethernet. Officially, the 10Base-T standard is IEEE 802.3u. Like Ethernet, 10Base-T is based on the CSMA/CD LAN access method.
AppleTalk	Inexpensive LAN (local area network) architecture built into all Apple Macintosh computers and laser printers. AppleTalk supports Apple's LocalTalk cabling scheme, as well as Ethernet and IBM Token Ring. It can connect Macintosh computers and printers, and even PCs if they are equipped with special AppleTalk hardware and software.
Asset	Component of a business process. Assets can include people, accommodation, computer systems, networks, paper records, fax machines, etc.
Availability	Ability of a component or service to perform its required function at a stated instant or over a stated period of time. It is usually expressed as the availability ratio: the proportion of time that the service is actually available for use by customers within the agreed service hours.
Availability Management	To ensure that ICT services are available for use consistently as agreed.
Bandwidth	The amount of data that can be transmitted in a fixed amount of time. For digital devices, the bandwidth is usually expressed in bits per second (bps).
Baseline	A snapshot or a position which is recorded. Although the position may be updated later, the baseline remains unchanged and available as a reference of the original state and as a comparison against the current position.
Bridge	A device that connects two LANs (local area networks), or two segments of the same LAN that use the same protocol, such as Ethernet or Token Ring.
Buffer	A temporary storage area, usually in RAM. The purpose of most buffers is to act as a holding area, enabling the CPU to manipulate data before transferring it to a device.
Build	The final stage in producing a usable configuration. The process involves taking one or more input configuration items and processing (building) them to create one or more output configuration items (eg software compile and load).
Capacity	Ability of available supply of processing power to match the demands made on it by the business, both now and in the future.
Capacity Management	To ensure that all ICT processing and storage capacity provision match present and evolving needs.
Category	Classification of a group of configuration items, change documents, incidents or problems.
Change	The addition, modification or removal of approved, supported or baselined hardware, network, software, application, environment, system, desktop build or associated documentation.

Change Management	The managed and recorded introduction of changes to hardware, software, services or documentation to minimise disruption to ICT operation and maintain accurate configuration information.
Client	The client part of a client/server architecture. Typically, a client is an application that runs on a personal computer or workstation and relies on a server to perform some operations. For example, an email client is an application that enables you to send and receive email.
Client/server architecture	A network architecture in which each computer or process on the network is either a client or a server. Servers are powerful computers or processes dedicated to managing disk drives (file servers), printers (print servers) or network traffic (network servers). Clients are PCs or workstations on which users run applications. Clients rely on servers for resources such as files, devices and even processing power.
Configuration management database (CMDB)	A database which contains all relevant details of each ICT asset, otherwise known as a configuration item (CI), and details of the important relationships between CIs.
Configuration Management	Implementing and maintaining up-to-date records of ICT hardware, software, services and documentation, and showing the relationships between them.
Definitive software library (DSL)	The library in which the definitive authorised versions of all software CIs are stored and protected. It is a physical library or storage repository where master copies of software versions are placed. This one logical storage area may in reality consist of one or more physical software libraries or filestores. They should be separate from development and test filestore areas. The DSL may also include a physical store (fire-proof safe, for example) to hold master copies of bought-in software. Only authorised software, strictly controlled by Change Management and Release Management, should be accepted into the DSL. The DSL exists not directly because of the needs of the Configuration Management process, but as a common base for the Release Management and Configuration Management processes.
Device	Any computer or component that attaches to a network.
Error trap	A signal informing a program that an event has occurred. When a program receives an interrupt signal, it takes a specified action (which can be to ignore the signal). Interrupt signals can cause a program to suspend itself temporarily to service the interrupt.
Ethernet	A LAN (local area network) architecture developed in 1976 by Xerox Corporation in co-operation with DEC and Intel. Ethernet uses a bus or star topology and supports data transfer rates of 10 Mbps. The Ethernet specification served as the basis for the IEEE 802.3 standard, which specifies the physical and lower software layers. Ethernet is one of the most widely implemented LAN standards.
FDDI (Fibre Distributed Data Interface)	A set of ANSI protocols for sending digital data over fibre optic cable. FDDI networks are token-passing networks, and support data rates of up to 100 Mbps (100 million bits) per second. FDDI networks are typically used as backbones for wide area networks.
Financial Management	To ensure that the ICT and technical resources are implemented and managed in a cost-effective way.

Firewall	A system designed to prevent unauthorised access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorised internet users from accessing private networks connected to the internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.
Gateway	A node on a network that serves as an entrance to another network. In schools, the gateway is the computer that routes the traffic from a workstation to the outside network that is serving web pages. In homes, the gateway is the ISP that connects the user to the internet.
Gigabit	When used to describe data transfer rates, it refers to 10 to the 9th power (1,000,000,000) bits. Gigabit is abbreviated Gb, as opposed to gigabyte, which is abbreviated GB.
HTTP (hypertext transfer protocol)	The underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the web server directing it to fetch and transmit the requested web page.
Hub	A connection point for devices in a network. Hubs are commonly used to connect segments of a LAN (local area network). A hub contains multiple ports. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets.
ICT	The convergence of information technology, telecommunications and data networking technologies into a single technology.
Incident	Any event which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in, the quality of that service.
Incident Management	To detect, diagnose and resolve ICT incidents as quickly as possible and minimise their adverse impact on normal operation.
ITIL	The OGC IT Infrastructure Library – a set of guides on the management and provision of operational IT services.
LAN	A computer network that spans a relatively small area. Most local area networks (LANs) are confined to a single building or group of buildings.
LocalTalk	The cabling scheme supported by the AppleTalk network protocol for Macintosh computers. Most local area networks that use AppleTalk, such as TOPS, also conform to the LocalTalk cable system. Such networks are sometimes called LocalTalk networks.
Logical topology	The logical topology is the way that the signals act on the network media, or the way that the data passes through the network from one device to the next without regard to the physical interconnection of the devices.
MAC (media access control) address	Each device on a network can be identified by its MAC address, a hardware address that uniquely identifies each node of a network. In IEEE 802 networks, the data link control (DLC) layer of the OSI reference model is divided into two sub-layers: the logical link control (LLC) layer and the MAC layer. The MAC layer interfaces directly with the network media. Consequently, each different type of network media requires a different MAC layer.

Management information base (MIB)	A management information base (MIB) is a database of objects that can be monitored by a network management system. Both SNMP and RMON use standardised MIB formats that allow any SNMP and RMON tools to monitor any device defined by a MIB.
Network	A group of two or more computer systems linked together. The two types of computer networks of interest to schools are LANs (local area networks) and WANs (wide area networks).
Network interface card (NIC)	A network interface card (NIC) is an expansion board inserted or built into a computer so that the computer can be connected to a network. Most NICs are designed for a particular type of network, protocol, although some can serve multiple networks.
Network traffic	The load on a communications device or system.
Node	A processing location. A node can be a workstation or some other device, such as a printer. Every node has a unique network address, sometimes called a data link control (DLC) address or media access control (MAC) address.
OSI reference model	The OSI (open system interconnection) model defines a networking framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, and proceeding to the bottom layer, over the channel to the next station, and back up the hierarchy.
Packet	A piece of a message transmitted over a packet-switching network. One of the key features of a packet is that it contains the destination address in addition to the data.
Packet switching	Refers to protocols in which messages are divided into packets before they are sent. Each packet is then transmitted individually and can even follow different routes to its destination. Once all the packets forming a message arrive at the destination, they are recompiled into the original message.
Peer-to-peer network	A type of network in which each workstation has equivalent capabilities and responsibilities. This differs from client/server architectures, in which some computers are dedicated to serving the others.
Physical topology	The physical layout of devices on a network. Every LAN (local area network) has a topology – the way the devices on a network are arranged and how they communicate with each other.
Port	In TCP/IP and UDP networks, an endpoint to a logical connection. The port number identifies what type of port it is. For example, port 80 is used for HTTP traffic.
Problem	The underlying cause of an incident or incidents.
Problem Management	The detection of the underlying causes of incidents and their resolution and prevention.
Protocol	An agreed format for transmitting data between two devices.
Protocol stack	A set of network protocol layers that work together. The OSI reference model that defines seven protocol layers is often called a stack, as is the set of TCP/IP protocols that define communication over the internet.

Proxy server	A server that sits between a client application, such as a web browser, and a real server. It intercepts all requests to the real server to see if it can fulfil the requests itself. If not, it forwards the request to the real server.
Release Management	To plan, test and manage the successful implementation of software and hardware. To define release policy and to ensure that master copies of all software are secured centrally.
Remote monitoring (RMON)	Remote monitoring (RMON) is a network management protocol that allows network information to be gathered at a single workstation. For RMON to work, network devices such as hubs and switches must be designed to support it.
Request for change	Form or screen used to record details of a request for a change to any CI within an infrastructure, or to procedures and items associated with the infrastructure.
Router	A device that forwards data packets along networks. A router is connected to at least two networks, commonly two LANs (local area networks) or WANs (wide area networks) or a LAN and its ISP's network. Routers are located at gateways, the places where two or more networks connect.
Segment	A section of a network that is bounded by bridges, routers or switches. Dividing an Ethernet into multiple segments is one of the most common ways of increasing available bandwidth on the LAN.
Server	A workstation or device on a network that manages network resources. For example, a file server is a computer and storage device dedicated to storing files. Any user on the network can store files on the server. A print server is a computer that manages one or more printers, and a network server is a computer that manages network traffic. A database server is a computer system that processes database queries.
Service Continuity Management	To minimise the impact on ICT service of an environmental disaster and put in place and communicate a plan for recovery.
Service Desk	The single point of contact within the school for all users of ICT and the services provided by Technical Support.
Service level agreement	Written agreement between a service provider and the customer(s) that documents agreed service levels for a service.
Service Level Management	The process of defining, agreeing and documenting required service levels and ensuring that these levels are met.
Simple network management protocol (SNMP)	A set of protocols for managing complex networks. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in management information bases (MIBs) and return this data to the SNMP requesters.
Star topology	A LAN (local area network) that uses a star topology in which all nodes are connected to a central computer. The main advantages of a star network are that one malfunctioning node does not affect the rest of the network and that it is easy to add and remove nodes.
Switch	A device that filters and forwards packets between segments of a LAN (local area network). Switches operate at the data link layer (layer 2) and sometimes the network layer (layer 3) of the OSI reference model and therefore support any packet protocol.

TCP/IP (Transmission Control Protocol/Internet Protocol)	The suite of communications protocols used to connect hosts on the internet. TCP/IP uses several protocols, the two main ones being TCP and IP.
Token ring	A type of computer network in which all the computers are arranged (schematically) in a circle. A token, which is a special bit pattern, travels around the circle. To send a message, a computer catches the token, attaches a message to it, and then lets it continue to travel around the network.
Topology	The shape of a LAN (local area network) or other communications system. Topologies are either physical or logical.
User datagram protocol (UDP)	A connectionless protocol that, like TCP, runs on top of IP networks. Unlike TCP/IP, UDP/IP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network. It is used primarily for broadcasting messages over a network.
WAN	A computer network that spans a relatively large geographical area. Typically, a wide area network (WAN) consists of two or more LANs (local area networks). Computers connected to a wide area network are often connected through public networks, such as the telephone system. They can also be connected through leased lines or satellites. The largest WAN in existence is the internet.
Workstation	Any computer connected to a LAN (local area network).