



Information Technology & Systems

Purpose / Summary

This document provides guidance and instruction to ensure that customer Service Desk tickets within Information Technology & Systems teams are dealt with in a consistent, auditable manner.

The policy statements in this document lay out the principles by which UWTSD will be governed whilst the procedures document the steps to be taken by UWTSD Information Technology & Systems staff when recording, acting upon and resolving Incidents, Service and Enhancement Requests and User Queries.

Following the procedures will ensure that working practices are auditable, can be benchmarked against industry standards and, where necessary, are able to be improved in line with UWTSD business needs. Such an approach will also enable UWTSD Information Technology & Systems to demonstrate the value that it provides to its customers and to plan for and resource future growth.

Document Control

Version	Author	Issued	Reason	Distribution List
1	James Cale	09/12	First draft	Info Serv SMT
1.1	James Cale	16/10/12	Second Edit	Info Serv SMT
1.2	James Cale	17/01/13	Third edit	Info Serv SMT
1.3	James Cale	19/02/14	Updated for SM	IT&S Swansea team
1.4	Ben Thorn	16/06/16	Updated Job Titles & Roles	IT&S

SIGNOFF:

Role	Name	Signature	Date

This page is deliberately left blank

Table of Contents

1	Introduction	1
2	Purpose of the Policies, Process & Procedures.....	1
3	Scope	2
4	Ownership& Responsibilities	2
5	Policy Statements	2
5.1	Basic Principles	2
5.1.1	Dos and Don'ts	3
5.2	Recording Policy	4
5.3	Prioritisation Policy.....	4
5.4	Response Policy	5
5.5	Resolution Policy	5
5.6	Closure Policy	5
5.7	Reporting Policy.....	6
6	Process Models & Activity Descriptions	6
6.1	Normal Office Hours - Times.....	6
6.2	Outside Normal Hours - Times.....	6
6.3	Process Documentation Layout	6
6.4	Process Flow; Normal Office Hours	7
6.5	Activity Descriptions; Office Hours	8
7	Prioritisation, with Response, Update & Resolution Targets	12
7.1	Incidents	12
7.2	Requests	13
8	P1 Incident Additional Requirements	13
8.1	General Information	13
8.2	P1 Incident Log.....	13
9	Management Control	14
9.1	Best Practice Guidance for Management.....	14
9.2	Assignment & Escalation	14
10	Roles in Incident Management	16
11	Handover Criteria.....	17
12	Example Categories.....	18
13	Example Change Schedule (optional).....	20
14	Structure & Location of Other Supporting Documentation	20
15	3rd Party Contact Guide	21
16	Email Contact Groups & Lists	24
17	Audit.....	25
17.1	Tailored ISO/IEC 20000 Question Set.....	25
18	Glossary of Terms	27

1 Introduction

UWTSD Information Technology & Systems has agreed and published objectives for dealing with all types of user Service Desk tickets in a timely and orderly manner to facilitate the attainment of business objectives by the university. (See section 7, Prioritisation with Response, Update & Resolution targets). The policies, process and detailed procedures laid out in this document are intended to provide a structure to ensure that UWTSD Information Technology & Systems not only achieves its published and agreed objectives, but can prove that they have been achieved. There are three general areas addressed in this document:

- The policies set out a set of basic principles formulated and to be enforced by Information Technology & Systems management to direct and limit their actions in pursuit of its goals.
- The process models how the principles will be implemented. It is a mandatory process and variation from this process is not permitted without the explicit permission of the Executive Head of Information Technology & Systems .
- The procedures provide activity descriptions which are intended to clarify the steps to be performed for each type of user contact. The process models show the sequence of, and iteration between, the steps to be performed. The activity descriptions give more detail about each step. Where appropriate, the descriptions reference further sections which are included to show exactly what is required in each step.

A Glossary of Terms is provided at Section 18.

2 Purpose of the Policies, Process & Procedures

The University of Wales Trinity Saint David is going through a period of transition; Information Technology & Systems must facilitate the business plans and continue to support the organisation. It is important that Information Technology & Systems is not only effective and efficient, but is demonstrably effective and efficient.

The purpose of the policies and associated procedures is to ensure that Information Technology & Systems actions can be reviewed regularly for improvement and can be audited to demonstrate the value that is provided to the customer by the actions of Information Services. The implementation of the policies and associated procedures is mandatory, so that Information Technology & Systems can be consistent in its handling of user tickets. This will enable Information Technology & Systems to handle tickets consistently across all locations and:

- Demonstrate the value provided to the University
- Improve, where necessary, the handling of user tickets and minimise/remove dissatisfaction and complaints
- Align IT activities to real-time University priorities so that we grow alongside the University because we are measurably the best
- Identify any required improvements in user training.

The implementation of policies and procedures may be seen by some as the imposition of additional work and putting additional bureaucracy in place of efficiency; it is, however, necessary in order to reduce unplanned labour costs and to enable management to determine where additional resources may be required.

3 Scope

The application of the policies and the execution of the processes and procedures laid out in this document are mandatory for all Information Technology & Systems staff dealing with any user contact, including all incidents and/or service requests (of any priority) during:

- Initial contact and recording
- Follow up contact (whether initiated from the user end or from Information Services)
- Resolution actions
- Closure
- Further investigation (including problem management)
- Final review
- Maintenance of associated documentation and records.

4 Ownership & Responsibilities

The Head of Information Technology & Systems is ultimately accountable for the quality of service provided and is therefore the owner of the policies and the process and is therefore responsible for undertaking actions) to ensure that it is being performed as intended.

It is the responsibility of all Information Technology & Systems staff (without exception) to comply with the policies and to execute the associated processes in a professional manner.

Section 10, Roles in Incident Management, shows where specific responsibilities lie.

5 Policy Statements

The process defined in this document details the steps to be taken when dealing with incidents. There may be circumstances where certain activities cannot be performed or have to be performed in a different way to how they are documented; however, any Information Technology & Systems staff undertaking any activities must adhere to the policies, principles and procedures in the following sub-sections.

5.1 Basic Principles

There are 5 basic principles to be applied when managing incidents via the Service Desk:

1. **Get sufficient information up front.** 1st line support must be able to prioritise tickets and both 1st and 2nd line support will need to determine how to resolve them. Although not all of the information detailed in the process step will be required for all incidents, it is far more disruptive to have to keep returning to the initiator to gather additional items of information that could have been gathered up front.
2. **Make sure you know that which has been agreed.** The prioritisation document at section 10 shows the main targets to work towards. The targets not only cover resolution times, but also response, assignment/escalation and update times.
3. **Assign or re-assign tickets and escalate issues before it is too late.** A target (see principle 2, above) is a point by which to aim to complete the work, not a point at which to start work. Tickets should be assigned with sufficient time remaining to for resolution in target and management issues must be escalated immediately.
4. **Accept that the originator of the ticket may know more than 1st or 2nd line support.** They are closer to the issue and are actually feeling the symptoms; they

also know exactly what was being done at the time of the incident and this sort of information must be captured accurately (see principle 1, above) and not assumed.

5. **Say “yes” when you should, but say “no” when you need to.** The Service Desk exists to provide service and should provide assistance wherever feasible. However, “casual” tickets and that which should be background work should never take precedence over assigned tickets and higher priority tickets.

5.1.1 Dos and Don'ts

When working on the Service Desk:

Do	Don't
Review the open queue when available for incidents waiting to be addressed. At least one member of each team must review the queue. The manager of each team is accountable for allocating this responsibility.	Wait for an incident to be assigned or to be approaching its target resolution time.
Use the defined Information Technology & Systems standards for formats and storage locations when creating documentation about business, IT and Service Desk issues for sharing.	Put knowledge files in personal databases or directories that are unknown to others.

When dealing with an incident:

Do	Don't
Record everything required as close to the actual time of the action as is feasible. A significant delay in recording means that information will be lost.	Assume that others will update records with your actions or delay recording un-necessarily. Either way, information needed for learning and improvement will be lost.
Record actions with clear and meaningful, but concise, explanations.	Use terms such as “fixed” or other simplistic words that convey nothing of value.
Ensure records are complete and include not only actions, but also the reasons for and results of those actions.	Just record “server re-booted” if the reason for the reboot was to deploy an installed OS component necessary to enable business function to be restored.
Provide regular feedback to 1 st line or to the business as appropriate, given the priority of the issue and the target timescale.	Assume that the business user is content not to have any information just because the target resolution time is still some way off.
Work through an incident all the way to resolution or ensure that it is properly handed over (reassigned) if at the end of your working day or will be out of the office. (Handover guidance is given at Section 11, Handover Criteria).	Be distracted by other tasks unless they are quite clearly of higher priority.

5.2 Recording Policy

A ticket may be initiated by an Information Technology & Systems member of staff or by a user. All tickets must be recorded in the Service Desk software. The aim of recording is to provide an audit trail and the record should, as a minimum, provide evidence of:

- The time of the contact
- The identity and contact details of the party initiating the ticket
- The action taken
- The time the action was taken
- The reason that the action was taken
- The result of taking the action.

If such evidence is not provided, then management will not be able to measure the workload and value provided and will not be able to plan appropriate resourcing levels.

Where issues are assigned or escalated, the record must reflect:

- To whom the issue was assigned or escalated
- The time of assignment or escalation
- The purpose of the assignment or escalation.

All recorded statements should be meaningful and be able to be understood by any interested stakeholders when reviewing the records. Another Information Technology & Systems member of staff should be able to look at the record in the future and know exactly what was done, why it was done and what was the result of doing it.

5.3 Prioritisation Policy

All tickets will be prioritised according to the current instructions documented and managed by the Executive Head of Information Technology & Systems. (Section 7, Prioritisation with Response, Update & Resolution Targets, contains the current instructions). Information Technology & Systems staff should respond to and attempt to resolve all incidents and requests in accordance with those instructions. Incidents prioritised as P1 or P2 will be assigned to specific Information Technology & Systems members of staff to resolve. The IT&S Senior Leadership Team are responsible for organising and balancing workloads of their team where sufficient resource is not available to deal with the number of incidents requiring actions. Incidents initially prioritised as P3 but not resolved within 2 working weeks will be promoted to P2 and assigned to a specific Information Technology & Systems member of staff for resolution whenever workload allows.

All issues will be addressed in priority order, with incidents taking precedent over requests. If lack of action on a request leads to (or is likely to lead to) a user being unable to work, it will be re-classified as an incident. If the user affected by the issue can continue to work, it should remain as a request.

5.4 Response Policy

Service Desk tickets can be raised via the Service Desk Software, Email, Telephone and where appropriate in person. The Service Desk administrators are in the main responsible for the logging of tickets that are generated through the email queue and via the Telephone. They are also ultimately responsible for assigning tickets manually logged by users that will sit in the open queue. The Service Desk team will assume these duties when the Service Desk administrators are not available. All Information Technology & Systems staff can log tickets made via in-person contact but where possible users should be encouraged to avoid this method of logging calls and to go through the central Service Desk.

The Information Technology & Systems member of staff to whom the issue has been assigned must respond to each incident and request submitted (via Service Desk Software, Email or Telephone) with a clear and meaningful explanation of what is happening and what the user should expect in terms of actions, contact and resolution. The response should always be through the Service Desk where possible as the logging of calls will automatically send a user a Service Desk update email confirming the ticket is opened. In some instances it may also be done via, by telephone or in person. But **any** communication through email, telephone or in person **must** also be documented in the Service Desk ticket.

For telephone or for face-to-face contact relating to P1 incidents, the Information Technology & Systems member of staff in contact with the user must respond at the time with clear and meaningful information, as above. If actions or timescales are unclear at the time of the contact, the Information Technology & Systems member of staff who determines the actions and timescales must make the response within the timescale specified in the current instructions.

It must be noted that where possible all UWTSD staff Service Desk calls should be logged via the Service Desk software. Any telephone or personal contacts to log a non-P1 call will require the Information Technology & Systems member of staff to inform the customer to follow the correct procedure for logging tickets which is via the Service Desk software.

5.5 Resolution Policy

The incident or request status may be set to “completed” by the Information Technology & Systems member of staff who has undertaken the resolution actions and also checked with the business or affected user, where it is necessary to do so. To mark an issue as completed, the Information Technology & Systems member of staff must record:

- The action taken to resolve the issue
- The reason for the action
- The outcome of the action
- The time of the action

5.6 Closure Policy

The incident or request can only be set to “closed” when the member of staff who logged the call has confirmed with the business/user that they give their consent for it to be closed. As part of the Service Desk software an automated email is sent to the user for them to confirm if the incident or request has been addressed (status of *completed* or *resolved*), if so the call status is set to *closed*. If the user believes it has not been resolved the call is reopened. The user has 5 working days to confirm resolution or the call automatically becomes *closed*.

5.7 Reporting Policy

The IT&S Senior Leadership Team will provide monthly reports to the Executive Head of Information Technology & Systems, detailing from their team (amongst other required elements):

- All incidents and requests not responded to within the designated time-scale, with reason
- All incidents and requests not resolved within the designated time-scale, with reason
- All incidents and requests currently being actioned and to whom they have been allocated
- Incidents and requests resolved but not yet closed, with reason
- Incidents and requests closed within designated time-scale.

6 Process Models & Activity Descriptions

The following sub-sections define the user ticket handling process and cover the recording of, actions required for and resolutions of:

- Incidents, whether P1, P2 or P3
- Service requests, whether R1 or R2, including;
 - User queries
 - Enhancement requests

Where time and workload allows, user queries will be dealt with by a 1st line Information Technology & Systems member of staff. Other tickets may be dealt with at 1st line, assigned to 2nd line or put in the open queue to be picked up by 1st or 2nd line Information Technology & Systems staff as workload allows.

6.1 Normal Office Hours - Times

Normal office hours are between 08:45 and 17:00 Mon – Thursday and 08:45 – 16:30 on a Friday (excluding Bank Holidays) by all Information Technology & Systems staff.

The process for normal office hour's support is detailed below (sub-section 6.4 and 6.5).

6.2 Outside Normal Hours - Times

There is currently no out-of-hours support, the only available out-of-hours process is during an emergency situation and is only for use when there is a physical risk to Information Technology & Systems equipment such as fire, flood or theft.

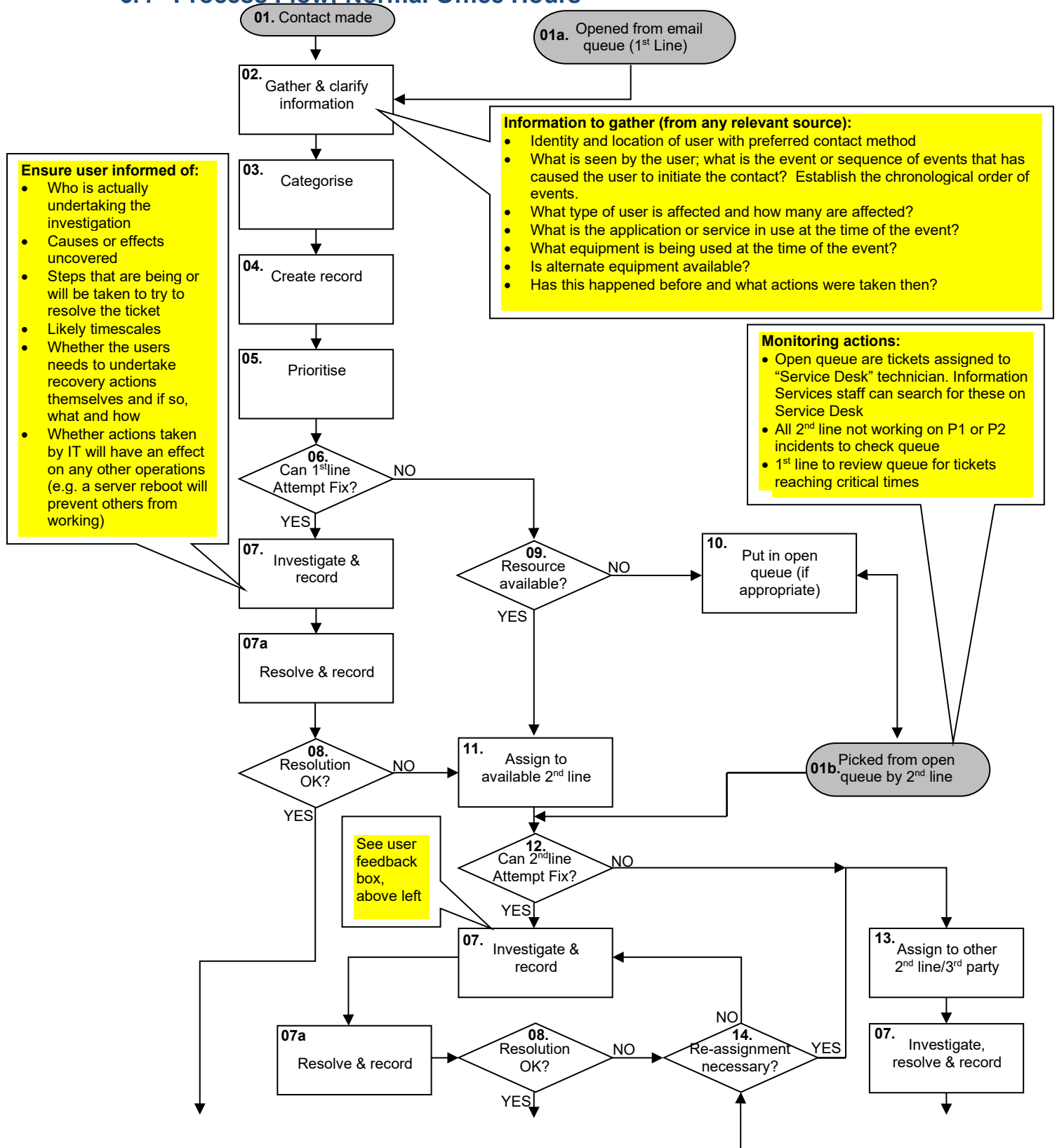
The Executive Head of Information Technology & Systems and Heads of Departments within IT&S are contactable in the event of the above.

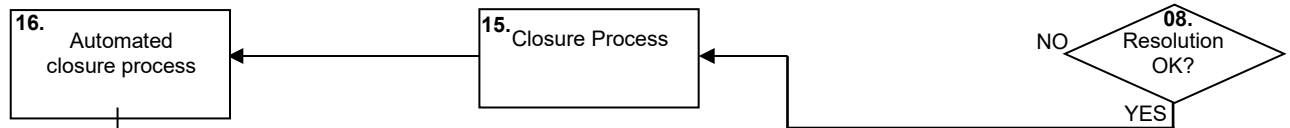
6.3 Process Documentation Layout

Each process is defined in overview in the first sub-section by a flowchart which shows the individually-numbered steps in the process. The start and end points of the processes are shown on the flow charts as grey terminators. The numbers on the flowchart relate to the activity descriptions contained in the subsequent sub-section which give details of each step shown on the flowchart.

Where further information is required for an activity description (such as a contact-out list or a document template), the additional information is shown in an appendix referenced in the activity description under the heading "comments".

6.4 Process Flow: Normal Office Hours





6. Activity Descriptions; Office Hours

No.	Title	Description	Comment
01	The first three activities are the three ways that in which the process can be initiated		See section 9; management control
	Contact made	Initial contact initiated by a user, if not made via Service Desk software will be via email, a telephone contact or by a personal visit. An Information Technology & Systems member of staff may also initiate at this point following a system alert.	
	01a Opened from email queue (1 st Line)	Tickets sent via email will be logged by the Service Desk administrators or by a 1 st line Information Technology & Systems member of staff.	
	01b Picked from Open Queue (2 nd Line)	All Information Technology & Systems staff will, as work allows, review the open queue and pick tickets for action. The service desk administrators and service desk engineer will each review the open queue and, where necessary, assign tickets at least at early morning, mid-morning, early afternoon and late afternoon. If any ticket remains in the open queue beyond its agreed resolution time, then the issue will be escalated to the Executive Head of Information Technology & Systems .	
The subsequent activities are broken down into detailed sequential steps for the purpose of clarity. In reality, an Information Technology & Systems member of staff will often perform several steps either together or in such rapid succession that they may not be seen as separate steps. As long as the intents of each step (accuracy of information gathered, clarity of recording and correct quality of decision making) are achieved, the steps should be performed as expediently as is feasible.			
02	Gather & clarify information	The first information to gather is whether what is being reported is: • An incident • A service request • A user query Minimum information required for all tickets: • Identity and location of user • What business activity is/could be affected • Service and/or component at the core of the issue. Where the user is reporting an apparent failure, the following should also be established: • Activity being performed by the user at the	Ensure that specific examples and statements are gathered; details of actions taken and process documents followed, appropriate asset tags etc.

		time that the issue became apparent Steps already taken by the user or by other parties to deal with the issue	
No.	Title	Description	Comment
03	Categorise	Select a category, sub-category and (where necessary) base category for the ticket. (Note that enhancement requests and user queries have a limited choice of available categories)	See section 12; <i>Tool categories</i>
04	Create Ticket	All tickets must be recorded in the Service Desk software to enable: - Reporting and analysis - Planning for future enhancements - Planning for future staffing	
05	Prioritise	Incidents must be prioritised as either: - P1 – adversely affecting strategic operations - P2 – adversely affecting multiple users - P3 – adversely affecting a single user. All other tickets will be prioritised as either: - R1 – requiring action - R2 – requiring planning	See section 7; <i>prioritisation, with response, update and resolution targets</i>
06	Can 1 st line attempt fix?	The 1 st line Information Technology & Systems member of staff recording the ticket should determine whether they can deal with the issue or if it should be assigned to another Information Technology & Systems member of staff. If the ticket is to be assigned, then go to activity09.	
07	Investigate & record	Investigation should centre around analysis of: - Information recorded so far - Previous incidents - The Information Technology & Systems knowledge base If the investigating Information Technology & Systems member of staff discovers or uses information that is helpful in the investigation and that is not recorded anywhere else, the Information Technology & Systems member of staff should record the information in the knowledge base on s:\Information Services\Knowledge Base. The recording of the investigation must include recording: - Actions taken	See section 13; <i>example change schedule</i> <u>NB:</u> P1 incidents require management escalation and additional monitoring and communication. See section 7; P1 incident additional requirements

		- The reasons for the actions - The results of the actions. Records should be clear and meaningful to enable the organisation to learn and develop.	
No.	Title	Description	Comment
07a	Resolve & record	An incident may be marked as “completed” when the Information Technology & Systems member of staff dealing with the incident is happy that the infrastructure, systems and applications are running sufficiently well to enable the business to achieve its targets. If this is done by means of a temporary workaround or if the resolving Information Technology & Systems member of staff feels that more information is required, then a problem ticket should be raised. (See problem management process). If the ticket is successfully resolved by the 1st line Information Technology & Systems member of staff, then go to activity 16. If the resolution is made by 2nd line or by a 3rd party, then go to activity 08.	<i>“Completed” means that the Information Technology & Systems member of staff is sure that the infrastructure and/or application is in a normal state and that the user should now be able to work normally.</i>
08	Resolution OK?	The Information Technology & Systems member of staff should check that the user is again able to perform their business tasks in an acceptable manner and then set the ticket status to “completed”. If resolution is not OK, then go to activity 14. (For an incident to be classified as “completed”, it is not always necessary for there to have been a permanent fix. Where a temporary fix has been made, it should be recorded as such so that it can be picked up later for appropriate action.)	<i>See section 7; prioritisation, with response, update and resolution targets</i>
09	Resource available?	If the 1st line Information Technology & Systems member of staff cannot attempt a fix, they should check to see if a resource is available to whom to assign the ticket. If the ticket is an incident prioritised as P1 or P2, then a resource must be found and workload re-organised if necessary.	<i>If there is no available Information Technology & Systems member of staff to deal with a P1 or P2 incident, then this must be escalated to management.</i>
10	Put in open queue (if appropriate)	Requests at either priority or incidents prioritised as P3 may, if resource is not currently available, be placed in the open queue to be picked up later. (See activity 01b). If any ticket remains in the open queue beyond its agreed resolution time, then the issue must be escalated to Executive Head of Information Technology & Systems .	<i>See section 9; management controls</i>

11	Assign to available 2 nd line	If a ticket is assigned to a 2nd line Information Technology & Systems member of staff, then the record should show: - To whom the ticket is assigned - The date and time of assignment. The Information Technology & Systems member of staff should also be informed of the response time and resolution target.	See section 7; <i>prioritisation, with response, update and resolution targets</i>
No.	Title	Description	Comment
12	Can 2 nd line attempt fix?	The 2nd line Information Technology & Systems member of staff to whom the ticket has been assigned should determine whether they can deal with the issue or if it should be assigned to: - Another 2nd line Information Technology & Systems member of staff - A 3rd party supplier. If the ticket is to be assigned, then go to activity 13, if not go to activity 07.	
13	Assign to other 2 nd line/3 rd party	If a ticket is assigned to a another Information Technology & Systems member of staff or to a 3rd party supplier, then the record should show: - To whom the ticket is assigned - The date and time of assignment. The Information Technology & Systems member of staff/3rd party should also be informed of the response time and resolution target. Go to activity 07.	See section 15; <i>3rd party contact-out guide</i>
14	Re-assignment necessary?	In the event of a 2nd line Information Technology & Systems staff or 3rd party being unable to resolve the incident, they should notify the Service Desk Engineer and either go back to activity 07 and re-investigate or go activity 13 and re-assign.	
15	Closure	When a 2nd line Information Technology & Systems member of staff or 3rd party has successfully resolved an incident or request and actions and times have been accurately recorded, the record status should be set to "Completed".	<i>"Completed" means that the technician is sure that the infrastructure and/or application is in a normal state and that the user should now be able to work normally.</i>
16	Automated	When an incident or request has been suitably	<i>"Completed"</i>

	closure process	resolved and set to “completed” the following automated process will run: - Email sent to user confirming issue has been resolved - User either agrees closure (call set to “closed”) or re-opens the call - User has 5 working days to respond before call set to “closed”. If agreement on closure cannot be reached, the record should be left as “completed” and the issue escalated to the Head of Information Technology & Systems for action.	<i>means that the technician is sure that the infrastructure and/or application is in a normal state and that the user should now be able to work normally.</i>
No.	Title	Description	Comment
17	End	The process is at an end when the ticket status is set to “closed”. If an agreement is not reached, it is the responsibility of the Head of Information Technology & Systems to decide whether to: - Keep the record open and re-investigate (activity 07) - Close the record - Open a new incident/request	<i>“Closed” means that records have been checked for and, where necessary updated to ensure, completeness and accuracy and that the user raising the incident has agreed to closure. If there is no response within 5 working days agreement may be assumed.</i>

7 Prioritisation, with Response, Update & Resolution Targets

These targets have been agreed with the business customer to ensure that business disruption is kept to a minimum. All targets are in working hours.

The Service Desk Engineer, IT and IS Manager will, each week, investigate all incidents and requests in their teams where targets have not been met and provide an exception report to the Head of Information Technology & Systems with an outline of actions required to ensure targets should be met in the future.

7.1 Incidents

Priority	Description	1 st Response target	Updates required	Resolution target
P1	Business operations halted or seriously affected; multiple sites, many users	30 minutes	Every 30 minutes	4 hours

P2	More than one users work significantly impacted; one site, multiple users	4 hours	As available	8 hours
P3	Single user affected	3 working days	As available	5 working days

7.2 Requests

Priority	Description	1 st Response target	Updates required	Resolution target
R1	Requiring action. E.g. User Access Request, add distribution group etc.	3 working days	None	5 working days
R2	Requiring planning. E.g. enhancements etc.	5 working days	As individually agreed	As individually agreed

8 P1 Incident Additional Requirements

8.1 General Information

P1 incidents take precedence over any other work being performed at the time. When dealing with P1 incidents within normal working hours, the ticket must be escalated as soon as it is logged to (one of) the IT&S Senior Leadership Team.

In addition, the Information Technology & Systems staff(s) working on resolution must provide updates to their line manager every thirty minutes. These updates should be made by email, but if email is unavailable, then by phone or in person where possible.

A P1 incident log (see below) should be completed as information becomes available. When updates are available, the Service Desk should also be updated.

If a 3rd party company is involved in resolution of P1 incidents, they should be requested to provide a 3rd party incident report. If one is not available, then the Executive Head of Information Technology & Systems should be informed.

8.2 P1 Incident Log

This is the standard P1 Incident Log which must be completed by the Information Technology & Systems staff(s) working on any P1 incident.

P1 INCIDENT LOG	
Incident Number:	
Brief Description:	

Timeline:	
Date / Time	Action
Issues Raised:	
Root cause:	
Procedural issues:	
Outstanding actions:	*** IT IS VITAL TO DOCUMENT, BEFORE CEASING ACTIVITY, ANY ACTIONS REMAINING TO BE EXECUTED ***

9 Management Control

9.1 Best Practice Guidance for Management

There may be many incidents in the queue with the same priority level, so it will be the job of the service desk/incident management staff initially, in conjunction with managers of the various teams to which incidents are escalated, to decide the order in which incidents should be picked up and actively worked on. These managers must ensure that incidents are dealt with in true business priority order (based on the institutions Strategic aims and its business priorities) and that staff are not allowed to arbitrarily choose the incidents they will address.

9.2 Assignment & Escalation

It is part of the duties of the IT&S Senior Leadership Team to regularly monitor progress on incidents and requests during normal office hours. The Executive Head of Information Technology & Systems should be notified by appropriate means when there is either:

- An entry in the open queue which has not been picked up but is nearing its target resolution time (e.g. within 5 working days for a P3 incident or 5 working days for an R1 request)
- An assigned incident or request which has reached its target resolution but is not marked as "completed".

The Service Desk administrator as well as Service Desk staff will also monitor the open queue and incident progress at early morning, early afternoon and late afternoon. The IT&S Senior Leadership Team will allocate resource as available to dealing with these incidents and requests.

In the event that agreement cannot be reached, the Service Desk Administrators will inform the Executive Head of Information Technology & Systems by any appropriate means.

The IT&S Senior Leadership Team will also attempt to provide a monthly report to the Executive Head of Information Technology & Systems and to the teams, showing:

- Number of incidents dealt with, by Information Technology & Systems staff
- Number of incidents successfully resolved, by Information Technology & Systems staff
- Number of incidents and requests outstanding
- Number of incidents and requests not resolved within timescale, with reasons.

Monthly reports will also be produced and provided, summarising the time period.

The Executive Head of Information Technology & Systems will when possible investigate all incidents and requests where targets have not been met and provide a report to the IT&S Senior Leadership Team with an outline of actions required to ensure targets should be met in the future.

10 Roles in Incident Management

The matrix on the following page shows the required involvement of the Information Technology & Systems roles in incident management. The involvement is defined using the following codes:

- A = “Accountable for”. This means “required to justify actions” and is the role which will be held to account for the activity
- R = “Responsible for”. This means “required to undertake actions” and is the role which can perform the activity
- C = “Consulted about”. This means “information is sought from”. This is not “permission is sought from”; permission is only sought from the accountable role
- I = “Informed about”. This means “information is given to”; the information can be about actions, progress and/or results.

Role	Executive Head of Information Technology & Systems	Service Desk Admin's	Head of Department	IT Team	Service Desk /Helpdesk	IS/MIS Team
Activity						
Answering tickets	A	R			R	
Opening from email queue	A	R			R	
Picking from open queue	A	R	I/C	R	R	R
Assigning from contact	A	R	I/C	R/C/I	R/C/I	R/C/I
Assigning from open queue	A	R	C/I	R/C/I	R/C/I	R/C/I
Resolving issues	I	A/C (Depending on where assigned)			A/C	A/C
Completing issues	A	I	R	R	R	R
Monitoring utilisation	A/I	C	R	C	C	C
Reporting utilisation	I		R/A	I	I	I
Reviewing utilisation	A/R		I/C			

11 Handover Criteria

Where any Information Technology & Systems member of staff in any team is working on an unresolved incident or request at the end of their working hours, the following actions should be taken.

Priority	Timing	Actions
P1	Any	Ensure sufficient resource available and working, else stay until resolved
P2	Any	Ensure sufficient resource (will be) available to complete within target resolution time, inform resource and Line Manager, formal handover and leave; else stay until resolved
P3	> 6 hours to target	Suspend and leave
P3	< 6 hours to target	Inform User, suspend and leave
P3	< 2 hours to target	Inform User, inform Line Manager, suspend and leave
R1	> 4 hours to target	Suspend and leave
R1	< 4 hours to target	Inform Line Manager, suspend and leave
R2	> 4 hours to target	Suspend and leave
R2	< 4 hours to target	Inform Duty Manager, suspend and leave

12 Example Categories

User Category	Sub-category	Base Category
Account management	Staff Students	Create new account Reset password Permissions Storage space
Audio and Visual	Incident Request	Video Conference booking Translation equipment Lecture Room AV Filming requirement Editing Lecture Capture
Computing Environment	Desktop PC Laptop Mac Monitor Scanner Printer/MFD	Licensing Software issue Hardware issue Documentation Training Printing/Copying/Scanning issue Request
Communication and Collaboration	Email	Student Email Staff Email (Exchange) Quotas Calendar issue User Query Shared Mailbox New account creation Permissions on mailbox SPAM GroupWise
	Telephones	Hardware issue Training Documentation User query Request for new phone line Request for new phone
	Remote Access	Citrix Remote desktop WebDav DirectAccess
Learning and Teaching Technology	VLE	Moodle Turnitin PepplePad
	Loan Laptops	Hardware issue User query
Mobile Devices	Admin	Request new device Documentation Training User query
	Device	Calendar issue Hardware error Lost settings Mail not received SIM card error Will not switch on
Management Information	Student DataStatutory	Data request

Reporting	Internal reports and statistics External reports and FOI requests	HESA KIS SSRS Reporting System Other
Business Information Systems	Student Records (SITS) Accommodation System (Kinetics) HR & Payroll Estates Service Desk (Quantarc) LMS (Horizon) Online payment system (WPM) Finance System (BluQube) Timetabling (Celcat) Website (T4) VLE (Moodle) Reporting Services CCTV CRM Attendance Monitoring (Celcat) ID Card System	Access request User query Fault/Error message Update Security
Team Categories	Sub-category	Base Category
IT	Desktop	Application management Environment management Profile/user settings User personalisation SCCM
	Citrix	Application Client Hardware Misc. Profile Server Software
	Exchange	Client access Maintenance Server down Service down Storage group
	Network	ISA LAN Proxy VPN WAN Wireless
	Storage	Folders/files maintenance Maintenance SAN hardware
IS	Software	Application Configuration Database Interface O/S

13 Example Change Schedule (optional)

The change schedule is maintained by the Head of Information Technology & Systems and shows the following information for each day over a 14 day period and for this and the subsequent period.

For each day and date:				
Change Number	Description	Actioned by	Status	Time
For each time period:				
Summary of scheduled changes to be confirmed				
Change Number	Description	Actioned by	Status	Time

14 Structure & Location of Other Supporting Documentation

Information Technology & Systems Knowledge Base is stored on s:\Information Services\Knowledge Base

All documents are to be in PDF format and follow the basic Information Technology & Systems document template that is also stored in the above location.

15 3rd Party Contact Guide

Phone system & ISDN Lines (except London hardware) Talk Talk Business Phone: 0800 298 2883 a/c: 077 00164574 Base phone numbers: 01267 676600 (Carmarthen) 01570 424700 (Lampeter) 01267 245600 (Y Llwyfan) 0207 566 7600 (London)	London phone system hardware PSU Technology Ltd phone: 0845 491 0050 contract: 11870	ICL 1Gb/s data link Talk Talk Business phone: 01635 573300 a/c: TRI040
Y Llwyfan Internet connection BTNet phone: 0800 699 879 circuit id:BTWE302907 PIP:505342 service id:FTIP003043646	JA.NET Phone: 0300 300 2212 E-mail:operations@ja.net	Pugh Computers Ltd Denver House Llanon Aberystwyth Wales SY23 5LP Phone: 01974 200201
European Electronique Ltd, Forward House, Oakfields Ind. Est, Eynsham, Oxon, OX29 4TT Dave Castle Dave.Castle@euroele.com Phone: 01865 883300	Phoenix No. 2 Golden Cross, 220 Chester Street Aston Birmingham B6 4AH Mark Potter Mark.Potter@phoenix.co.uk Phone: 0844 863 1320 Phone: 07713 654909	RM RM EDUCATION PLC NEW MILL HOUSE 183 MILTON PARK OX14 4SE Support Phone: 0845 404 0000

Stone Computers Ltd Granite One Hundred Acton Gate Stafford Staffordshire ST18 9AA support@stonegroup.co.uk Phone: 08448 80 23 66	OnLiTECH Limited Unit 2 Neates Yard Hungerford Berkshire RG17 0NB United Kingdom Carl Donovan sales@onlitech.com Phone: 01488 685223	IP Performance 1-3 Merietts Court Long Ashton Business Park Long Ashton, Bristol England, UK BS41 9LW Mike Baker mbaker@ip-performance.co.uk Phone: (0) 1275 393382
Konica Minolta Business Solutions Ltd. Axis 2, Axis Court, Mallard Way, Riverside Business Park, Swansea Vale, Swansea SA7 0AJ Robert Stanton robert.stanton@konicaminolta.co.uk Phone: 01792 795486	Starfish Tech Technologies Reading Enterprise Centre Whiteknights Road, Reading, Berks. RG6 6BU Peter Blatchford p.blatchford@starfish.tv Phone: 0870 132 6277	DataComplete Data Complete Limited 345, Llangyfelach Road. Brynhyfryd. Swansea. SA5 9LQ John Long john@datacomplete.co.uk Phone: 01792 465901
Synapse Communications 113 Station Road Ystradgynlais SA9 1PJ synapsecom@hotmail.com Arthur	PSBA Team Cefn Coed Business Park Parc Nantgarw Nantgarw Cardiff, CF15 7QQ psba.communications@uk.logicalis.com Phone: 0845 602 7155	XMA COMPUTER PRODUCTS Thomas House Wilford Industrial Estate RUDDINGTON LANE Wilford Nottingham NG11 7EP

Oxford Computer Group UK Park Farm Business Centre Middleton Stoney, Bicester, Oxfordshire OX25 4AL UK Alison.Werkman@oxfordcomputergroup.com Phone: 08456 584425	Microsoft Customer Support OLSRV.AEDU.WW.00.EN. CVG.PUN.TS.T03.ORA.SD.EM @css.one.microsoft.com	WVN Information Technology & Systems and Systems Swansea University Singleton Park Swansea SA2 8PP Phone: 0300 6880688 support@wvn.ac.uk
XMA XMA Wales Brecon House Suite 10 William Brown Close Llantarnam Business Park NP44 3AB Marie-Louise Hitt XMA Wales – HE/FE Manager xmawales@xma.co.uk		

16 Email Contact Groups & Lists

Email group for management alerting.

Title	Name	Email	Telephone
Executive Head of Information Technology & Systems	James Cale	j.cale@tsd.uwtsd.ac.uk	01267676754
Head of Service Delivery	Ben Thorn	b.thorn@uwtsd.ac.uk	01267225115
Head of IS&I	Matthew Marl	m.marl@uwtsd.ac.uk	01267676807

17 Audit

The Head of Information Technology & Systems will conduct occasional audits based on the international standard for service management, ISO/IEC 20000. The following sub-section shows the list of questions selected for these audits and the evidence required.

An occasional audit based on this standard may be conducted by an external consultant.

17.1 Tailored ISO/IEC 20000 Question Set

The following set of questions is based on the ISO / IEC standard for Incident Management and has been tailored for use in UWTSD IT. An auditor would not only seek an answer to each question (and to pass, every answer MUST be “yes”) but would require documentary evidence that the answer given is correct.

Audit Question		Comment
1	Are all Service Requests recorded?	<i>Within Service Desk software and identifiable as Incidents or Request</i>
2	Are all Incidents recorded?	
3	Is the reporting method well known throughout the University?	<i>Whom to contact, when, methods of contact etc.</i>
4	Is the reporting method, and are the associated procedures, well known throughout the University?	<i>A common understanding of the methods; a consistent approach to recording etc.</i>
5	Do the members of staff who record incidents have knowledge of/training in the business processes being supported?	<i>To at least gain an understanding of the user's perception of difficulties</i>
6	Do the procedures (4, above) define: Recording? Categorisation? Prioritisation? Escalation? Updating? Resolution? Closure?	<i>How to, format etc.</i> <i>Inc. sub and base as necc.</i> <i>Inc. review of priorities</i> <i>Functional & hierarchical & communication</i> <i>Appropriate information & communication</i>
7	Are the Users kept informed of the progress of Incidents and Requests that they have initiated?	<i>Both good and bad news</i>
8	Are Customers informed in advance and an action agreed if agreed resolution times cannot be met?	<i>As early as possible</i>

Audit Question		Comment
9	Do all staff involved in dealing with Incidents and Requests have access to information about: Known Errors? Current and historic Problems? Infrastructure components; their history and relationships with each other?	<i>And is the information in a consistent form and easy to access?</i>
10	Is the accuracy of such information checked as part of the ticket handling process?	<i>To provide on-going improvement and reduce reliance on "head-knowledge"</i>
11	Are required corrections resulting from the checks (10, above) actually made?	
12	Are Major Incidents classified and managed according to a defined process that is actually followed in practice?	<i>P1 – adverse event, risk registers</i>
13	Are service reports effective, accurate and timely?	<i>And read and acted upon?</i>
14	Is recorded Incident data generally suitable and of sufficient quality for use in Problem analysis?	<i>Accurate and sufficient detail</i>
15	Is information on all significant Incidents analysed to discover the underlying cause?	<i>P1/P2</i>
16	Does the recorded Incident information make it easy to identify recurring Incidents?	<i>And the percentage of workload that is recurring</i>
17	Is information on recurring Incidents analysed to discover the underlying cause?	<i>To reduce workload</i>

18 Glossary of Terms

UWTSD IT quality control documentation uses the following definitions.

Term	Definition
Accountable	A role defined as being accountable is the role that is literally “held to account”. Being accountable for something includes being required to justify it
Activity description	Where necessary, a set of documented detailed instructions to fully explain the mandatory steps in performing a <i>process</i> activity
Information Technology & Systems member of staff	A UWTSD IT employee or other person involved in the detection, recording or assignment of <i>issues</i>
1 st line	Service Desk staff
2 nd line	With the exception of the designated <i>1st line Information Technology & Systems member of staff</i> , all Information Technology & Systems member of staffs are deemed to be 2 nd line, including members of the IT and IS teams.
3 rd Party	A <i>supplier</i> or any external company that is, or will need to be, involved in providing a resolution to an <i>issue</i>
Assignment	Passing from <i>1st line</i> to <i>2nd line</i> , <i>2nd line</i> to another <i>2nd line</i> or <i>2nd line</i> to a 3 rd party <i>supplier</i> for action
Audit	A type of review carried out by a disinterested party based on checking evidence that an organisation has done and continues to do that which it claims to have done and to do
Contact	A telephone contact, email or personal visit to raise an issue
Customer	The business supported by UWTSD Service Desk
Designated duty manager	The Head of Information Technology & Systems is ultimately accountable for the process and is responsible for taking management action to ensure its effective execution. When the Head of Information Technology & Systems is not available for one day or more, the responsibility will be transferred to a designated duty manager who will inevitably be either the IT or IS manager.
Document	Evidence of intention. Required for audit purposes to show what an organisation should be doing. The documents will usually be in the form of <i>policy</i> , <i>process</i> and <i>activity description</i>
Enhancement	A request for an improvement to or extension of service, to be treated as a <i>Request</i> at <i>priority R2</i>
Escalation	Passing to management for decision
Follow-up contact	Any contact in any direction between an <i>Information Technology & Systems member of staff</i> and a user about an Incident or a <i>request</i> that has already been recorded. Follow-up contacts may be initiated

	by a <i>user</i> or by an <i>Information Technology & Systems member of staff</i>
Incident	Any reported/known event that has resulted in or may result in an interruption to or a reduction in quality of the IT service experienced by the <i>customer</i> or <i>user</i>
Priority P1	An Incident which halts or has a serious negative impact on business operations; an incident that affects multiple sites and/or many users
Priority P2	An incident which has significant negative impact on user's work; an incident that affects one site and/or multiple users
Priority P3	An incident that affects one <i>user</i> and does not negatively impact the business or site operations
Issue	A general term to cover any <i>incident</i> and/or <i>request</i> dealt with by an <i>Information Technology & Systems member of staff</i>
Known error	A known fault that has been analysed and assessed and for which at least a <i>workaround</i> exists and perhaps a permanent <i>solution</i> has been planned
Policy	Principles to be applied in order to achieve the aims of the organisation
Problem	The underlying cause of one or more incidents or even of a potential <i>incident</i>
Procedure	A documented <i>process</i> , showing activities, inputs and outputs
Process	The managed set of activities to be executed to achieve an objective
Record	Evidence of action. Required for <i>audit</i> purposes to show what an organisation is doing. The records will normally be held in Service Desk software and/or in the knowledge folder in the IT Service Desk, but may be paper-based, where appropriate
Responsible	A role being defined as responsible for something is the role required to undertake the actions to do it
Request	A request for an action to be undertaken rather than a report of a (perceived) failure
Priority R1	A request requiring short-term action
Priority R2	A request requiring longer-term action to be planned
Review	An assessment by interested stakeholders to determine whether what an organisation does is compatible with its aims and objectives
Solution	The action that means that the <i>problem</i> no longer exists and therefore prevents related incidents from re-occurring

Supplier	Any 3 rd party external company that is, or will need to be, involved in providing a resolution to an <i>issue</i>
Ticket	The information held within the Service Desk software that details any incident or requests. The ticket contains details of the incident or request as well as details of the user.
User	The customer who contacts the Service Desk or who is or may be affected by the issues being actioned by the Service Desk
User contact	Any contact between a business <i>customer</i> representative or <i>user</i> and the Service Desk or support teams, whether initiated by a <i>user</i> or by an <i>Information Technology & Systems member of staff</i>
Workaround	A way of enabling the <i>user</i> to continue to perform their duties without necessarily finding or fixing the underlying <i>problem</i>