
I.T. Department

Service Level Agreement

Version x.x

Table of Contents

1	Introduction
2	Parties of the Agreement
3	Summary of Services Covered
4	Our Responsibilities
5	Your Obligations
6	Core IT Systems
7	Hours of Support
8	Service Availability & System Uptime
8.1	Extended Availability or Support
8.2	Planned Maintenance
8.3	Emergency Maintenance
9	Security
9.1	Security Assessment of 3rd party suppliers
9.2	Assistance with completion of security questionnaires
9.3	User Access to Systems
9.4	Third Party Access Requests
9.5	Backing up your data
9.6	Your Security Responsibilities
9.7	Security and Anti-virus Patching
10	Faults and Problems
10.1	Contacting us
10.2	Communicating with you
10.3	Resolving Your Issue
10.4	Major Fault management
11	Requesting Changes
11.1	Raising Your Request
11.2	Prioritisation
11.3	Communicating with you
11.4	Urgent Requests
12	Service Requests
13	Procurement of IT Goods and services
14	Managing 3rd Party Suppliers
15	Disaster Recovery
16	Our Performance
17	Appendix 1 – Example KPI Report
18	Appendix 2 – Fault and Problem Definitions

1 Introduction

This document records the services provided by the central IT Department to support business operations at Canterbury Christ Church University. It defines the agreed levels of service you can expect to receive as well as your obligations as a service customer.

The agreement is formally reviewed at least once every 12 months and updated with any changes made to the services during the preceding year. The Director of IT is responsible for ensuring the review takes place.

2 Parties of the Agreement

This agreement is between the IT Department, represented by Celia Hardy, who is ultimately responsible for the delivery of the services described in this document, **AND** Canterbury Christ Church University's internal IT users and stakeholders, represented by the key stakeholders listed below.

Name	Role

3 Summary of Services Covered

This agreement covers the IT services listed in section 5 which are provided by the IT Department to all UK based Canterbury Christ Church locations.

The IT Department will:

Ensure that IT services are available for use when our users need them.

Protect Canterbury Christ Church University's electronic data, by keeping it secure and safe from unauthorised access.

Ensure that preventative maintenance activities are performed to keep everything fit and healthy.

Ensure that hardware and applications software remains current and in supported versions.

Provide solutions that enable our users to access the IT systems in a flexible and secure way.

Ensure that alternative solutions are available in the event of disasters.

Work with our colleagues to design and develop solutions that add value to Canterbury Christ Church's core business functions.

Provide help, advice, and support in the use of all centrally maintained IT services.

4 Our Responsibilities

We will provide the services and support as defined in this document.

We will deal with your requests in a consistent and fair manner.

We will communicate honestly and openly with you about the progress of your requests.

We will provide at least 3 working days notice of any planned maintenance activities which will affect service availability.

We will provide regular (monthly) information on our performance against the key performance indicators listed in this document.

5 Your Obligations

You will follow the guidance contained or referenced in this document and use our services in the way intended.

You or someone on your behalf will provide us with timely and good quality information with which to service your request when required.

You will help with prioritising your requests and be prepared to sponsor your requests.

You will make time to test and approve changes which we make on your behalf.

You will provide at least 2 working days notice of any activity that is likely to affect our ability to provide IT services.

If you are a manager of Canterbury Christ Church University staff, you will ensure that they are aware of their obligations and that they meet them

6 Core IT Systems Provided

Staff Facing

	System	Description	System Uptime	Service is available	Support is available	Key Business Stakeholder / deputy
1	XXXX	<ul style="list-style-type: none"> Front Office – Xxxx (CRM) Back Office – Xxxx Reporting 	99.9%	24 x 7	Mon – Fri 8am – 6pm	Xxx / Xxxx Xxxx, Xxxx Xxxx, Xxxx
2	Internet access	Access to the worldwide web for staff browsing and access to Internet based services.	99.9%	24 x 7	Mon – Fri 8am – 6pm	Xxxx
3	Email	Sending and receiving email to and from Canterbury Christ Church University.	99.9%	24 x 7	Mon – Fri 8am – 6pm	Xxxx
4	Telephone	Use of desk-based telephones with PC integration.	99.9%	24 x 7	Mon – Fri 8am – 6pm	Xxxx,Xxxx
5	Desktop Printing	Printing, photocopying and scan-to-email services integrated with CCCU security cards.	99.5%	24 x 7	Mon – Fri 8am – 6pm	Xxxx
6	Desktop	Access to IT services via a PC and including standard Microsoft Office applications.	99.9%	Mon – Fri 8am - 6pm	Mon – Fri 8am – 6pm	Xxxx
7	Remote Access	Secure remote access to XXXX IT systems from Windows PCs.	99.9%	24 x 7	Mon – Fri 8am – 6pm	Xxxx
8	Local Network	Connectivity within each CCCU location.	99.9%	24 x 7	Mon – Fri 8am – 6pm	Xxxx
9	Wide Area Network	Connectivity between CCCU locations and central IT services in the Data Centre or The Cloud.	99.9%	24 x 7	Mon – Fri 8am – 6pm	Xxxx
24	Internet	Filtering of Internet traffic for virus and Trojans and	99.9%	24 x 7	Mon – Fri	Xxxx

System	Description	System Uptime	Service is available	Support is available	Key Business Stakeholder / deputy
Filtering	enforce XXXX acceptable usage policy			8am – 6pm	
26	External hosted fax service.	99.5%	24 x 7	Mon – Fri 8am – 6pm	Xxxx
27	IT's Incident Management software.	99.9%	24 x 7	Mon – Fri 8am – 6pm	Xxxx
33	Bloomberg Connection to external service providing investment prices and standing data on XXXX Investments.	99.5%	Mon – Fri 8am - 6pm	Third Party Arrangement	Xxxx
35	Connection to externally hosted system containing information on XXXX employees and payroll data.	99.9%	24 x 7	Third Party Arrangement	HR (Xxxx)

7 Hours of Support

We provide support for all services between the hours of 8am and 6pm Monday to Friday (excluding UK Bank Holidays).

Support for systems using non CCCU-strategic technology or hosted elsewhere is provided on a best endeavours basis.

Although some services are available on a 24 x 7 basis we do not routinely provide support after 6pm or before 8am weekdays or anytime at weekends.

8 Service Availability & System Uptime

Service Availability is the time that the service is available to use. We have two categories,

Category 1 24 x 7	The service can be used all the time.
Category 2 Mon to Fri 8am – 6pm	The service is available for use during CCCU's core operational hours.

System uptime refers to the %age of time the service will be available during its supported hours. We provide two levels of uptime.

Level 1 99.9%	8.76	hours of unscheduled downtime per year
	43.2	minutes of unscheduled downtime per month
	10.1	minutes of unscheduled downtime per week
Level 2 99.5%	1.83	days of unscheduled downtime per year
	3.6	hours of unscheduled downtime per month
	50.4	minutes of unscheduled downtime per week

Pre-agreed downtime (e.g. for scheduled releases and planned maintenance) does not count in the calculation.

8.1 Extended Availability or Support

If you need an application, service or support to be available beyond the normal hours contact the IT Service Desk or raise a service request. We'd appreciate as much notice as possible to resource the necessary cover which will be provided on a best endeavours basis. Note that you may need to provide funding to cover additional staffing costs.

8.2 Planned Maintenance

We will provide at least five working days notice to the key stakeholders (defined in section 5) before carrying out planned maintenance or releases. Wherever possible, these activities will occur outside the normal service hours.

We will carry out planned releases for XXX and XXX on pre-arranged dates, Monday to Friday between 5am and 8am.

We will agree any exceptions to this with the key stakeholder (or their deputy).

8.3 Emergency Maintenance

Occasionally we need to carry out urgent maintenance to mitigate an immediate risk or issue. When this happens we will consult with the key stakeholders (listed in section 5) of the services affected, to verify the need for emergency action and to agree the maintenance window.

9 Security

We provide a range of security services, including:

9.1 User Access to Systems

Use XXX, available <http://xxx.html> to let us know what you need.

We will complete your request within 3 working days of receiving it.

9.2 Access Requests for Associates

Access to specific systems can be provided to 3rd parties for the purposes of support.

To make a new access request, follow the approval process managed by the HR Department. This will result in a system account being created for your Associate.

Once an account has been created and you require a change to the scope of access required, raise a service request for system access through the via

<http://xxx.html>

Access requests will be fulfilled within an hour of them being raised.

9.3 Backing up your data

We make sure that all centrally held data is backed up on a daily basis and a copy held off site.

Daily backups are created Monday to Friday and kept for 4 weeks.

Additional monthly backups are created every 4 weeks which are kept for 12 months

If you need to retrieve a file, folder or data from backup, lodge a service request via the IT Service Desk:

<http://livht01web01.XXXX.org.uk:8180/HeatWebUI/hss/HSS.html>

Requests will be dealt with according to the agreed priority.

Please note: that data held locally on laptops is not backed up. It is your responsibility to see that copies of important data are maintained on your Home directory (X?: drive).

9.4 Your Security Responsibilities

We expect you to comply with CCCU's policies and follow guidelines regarding the use of CCCU systems and handling of data. Non-compliance can impact the delivery of IT services to yourself or others.

The CCCU Data Security Manual?? is located at: <http://xxx.pdf>

The guidelines are located at: <http://xxx.pdf>

9.5 Security and Anti-virus Patching

Each month we make sure that all critical operating system and application patches are applied to servers and desktop computers.

10 Faults and Problems

10.1 Contacting us

The IT Service desk is your first point of contact with the IT department if you have an issue, fault or general query about IT services. If the issue is critical (see below) or you can not use the other methods you can contact us by

Telephone

2626 (internal)

01227 86 2626 (external)

We aim to answer your call within 3 rings

If we are unable to answer please select the option of a ring back, your call will keep its place in the queue and we will call you back when it reaches the top.

We aim to resolve your query or issue at first point of contact 70% of the time and if we cannot the call will be passed on to one of the IT support teams.

10.2 Communicating with you

Priority	Communication from Support team	Ongoing Updates
Critical (priority 1)	Within 15 minutes	Every hour
High (priority 2)	Within 1 working hours	As agreed with the user
Medium (priority 3)	Within 2 working hours	Updates will be provided through Heat Self Service.
Low (priority 4)	Within 2 working hours	Use Self Service to view updates

10.3 Resolving Your Issue

We will endeavour to resolve your issue within the target timeframe relevant to its priority:

Priority	Target Resolution Times
Critical (priority 1)	90% within 4 working hours
High (priority 2)	85% within 2 working days
Medium (priority 3)	80% within 5 working days
Low (priority 4)	80% within 20 working days

Service may be restored either by a work-around or by using a permanent solution. If a work-around is employed the priority of the issue will be reassessed and may change.

Where service is not restored within the target resolution times, we will discuss and agree an alternative timescale with you at the next status update.

10.4 Major Fault management

When major incidents occur, usually those that have been designated as business critical (Priority 1), we will assign a Major Incident Manager who will be responsible for co-ordinating the problem resolution and handling communication with key stakeholders affected.

11 Requesting Changes

This section applies when you need to make a change to existing functionality or IT services or to introduce new ones. It does not cover project work.

Projects are individually planned and the SLA for each one is included in its Project Initiation Document. Governance is in accordance with the IT project delivery process. <http://xxx.pdf>

11.1 Raising Your Request

Use xxxx to let us know what you need. If you need advice or help please contact the XXX Team on x1234.

We will contact you within two working days to confirm your request and let you know when it will be reviewed for future delivery. Note that if the request falls short of the minimum information required it will be returned to you.

11.2 Prioritisation

Prioritisation meetings are held regularly with key business stakeholders or their deputies, to agree the work that will be included in the next release of small changes.

Prioritisation is necessary to ensure that we are using our resources on the most important things as agreed by the business stakeholders.

11.3 Communicating with you

We will update you on the progress of your request after each review meeting until it is delivered or closed.

11.4 Urgent Requests

Urgent requests will be accepted into the current release wherever possible. This will usually require reprioritisation of items already in the release. You should be prepared to justify and possibly negotiate with the other stakeholders in the release to have your request included.

12 Service Requests

We use the term Service Request to refer to a request for one of the pre defined IT Services listed below.

Let us know about your service request by completing the online form available via

<http://xxx.html>

You will receive an automated acknowledgement soon after you have made your submission.

We will contact you within two hours of you raising a service request to agree when your work will be booked in our schedule.

Fulfilment time indicates the amount of effort needed to perform the task and does not include analysis and any purchasing lead times.

Examples of service requests

Service Requested	Typical lead time	Typical fulfilment Time
Standard Laptop	2 weeks	2 days
New user work station	1 week	½ day
Office Move (up to 4 desk positions)	1 week	½ day
Standard software installation	2 days	1 hour
Telephone (New / Amend / Delete)	1 week	½ day
Extended hours support or availability	3 days	n/a
Setup remote access	2 days	2 hours

13 Procurement of IT Goods and services

We are responsible for purchasing all IT related goods and services.

We aim to process all purchase requests and place the order for known & standard goods within 3 working days, once verified and subject to budget holder approval. Non standard purchases are likely to take longer, but we will advise you if this is the case.

You should submit your purchase request using the online facilities available

<http://.html>

or speak with your IT business partner for advice.

14 Managing 3rd Party Suppliers

We are responsible for managing the day to day delivery of IT services provided by 3rd parties.

We monitor their performance against agreed Service Level Agreements and hold regular review meetings with all key suppliers.

Where their performance does not reach the required standard we work with them to improve the service.

15 Disaster Recovery

In the event of a disaster and the CCCU business continuity plan being invoked the service standards contained within this agreement will no longer apply.

Full Business Continuity plans are held by the XXXX. Details of the plans are published [here](#).

We provide a disaster recovery service to support the BCP plans and depending on the scenario we are able to recover all systems described in section 6 IT Core Services to an alternative data centre within 4 hours of being invoked.

16 Our Performance

So that you can see how we are doing, every month we will publish our performance against the Key Performance Indicators listed in appendix 1. This information will be available [here](#).

Periodically we will also carry out surveys to understand your view on our performance. Please don't wait for the survey though; you can feedback at any time by speaking directly with any member of the IT Department management team. We welcome your feedback and aim to respond to all feedback received.

17 Appendix 1 – Example KPIs

I.T. MONTHLY KPI REPORT				
KPI	Priority / Item	Definition of Key Performance Targets	Actual	R/G
SERVICE REQUESTS				
1	Initial Response	90% in 2 working hours - (Remaining within 2 working days)	92%	
2	Completion	90% within agreed completion date	87%	
FAULTS AND PROBLEMS				
3	P1 – Critical	90% resolved within 4 working hours of being reported	100%	
4	P2 – High	80% resolved within 2 working days of submission	100%	
5	P3 – Medium	80% resolved within 5 working days of submission	80%	
6	P4 – Low	80% resolved within 20 working days of submission	80%	
7	Classroom emergency	90% attended within 10 minutes	95%	
CHANGES				
8	Initial Response	90% responded to within 2 working days of submission	30%	
9	Status Update	100% of open changes have had monthly status updates published	75%	
SYSTEM AVAILABILITY				
10	Desktop Services	99.9% service availability during the past month	100%	
11	Learning & Teaching Systems	99.9% service availability during the past month	90%	
12	Telephony	99.9% service availability during the past month	100%	
SECURITY				
13	Security Patching	95% of supported systems successfully patched in the past month	100%	

18 Appendix 2 – Fault and Problem Definitions

Faults and problems will be prioritised on the following basis:

Type	Criteria
Critical (P1)	Affecting the whole of CCCU's users and / or
	Affecting more than 1000 students and / or
	Is causing an immediate serious financial impact of £10,000 + and / or
	A regulatory breach has occurred. and / or
	There is a significant risk of reputational damage, e.g customer data exposed and / or
	There is an immediate risk to deadlines
High (p2)	Affecting a Team / Department in CCCU and / or
	Affecting 51-1000 students and / or
	Is causing an immediate serious financial impact of £10,000 + and / or
	There is likely to be a regulatory breach and / or
	Is likely to cause reputational damage e.g. customer data exposed and / or
	There is likely to be an imminent risk to deadlines
Medium (P3)	Affecting 1 CCCU User and / or
	Affecting 0-50 students and / or
	Is causing an immediate serious financial impact of £0 - £101 and / or
	There is no regulation breach and / or
	It could cause reputational damage and / or
	There is no risk to deadlines
Low (P4)	Relates to a question or aesthetic issue.
	There is no impact to service delivery.