SCHEDULE 2

DIGITAL REPOSITORY - APPLICATION SERVICE LEVEL AGREEMENT

CONTENTS

1 SERVICE OVERVIEW

The Service Provider's Digital Research Technologies team provide expertise and consultancy services to support a range of research and scholarly activities.

The service provides a hosted installation of the Service Provider's Digital Repository Solution with access to their professional support services.

This enables customers to access a secure, reliable, and scalable repository service without the need for internal specialist IT software or infrastructure resources.

The service adheres to Open Access Publishing and Open Data principles and as such enables institutions to move to the more open model of sharing repository data should they wish. This embraces and packages the latest offerings from the Open Source community along with the Service Provider's tailored utilities, configurations, and services.

In addition, customers can engage the Service Provider's Professional Services Group to tailor their repository to meet individual demands.

This service is ideal for Higher Education Institutions and other Research and Memory focused organisations (such as Clinical Charities or Museums). This provides the benefits of an industry proven repository with the peace of mind given by the expertise of the Service Provider's leading repository experts and the commercial reliability of the Service Provider's hosting and support services.

2 SERVICE DEFINITION

The Digital Repository Software as a Service provides the following key standard features

- The Service Provider's Digital Repository Solution
- Managed Hosting
- Service Management and Reporting
- Phone Support Desk 5*8 as standard
- Support Tracking system
- Access to the Service Provider's Support and Professional Services Teams
- Support and Consultancy Days Included
- Access to Customisation Services
- Service Level Agreement

The initial Implementation of this Service is subject to separate agreement and is dependent on the specific customer requirements.

3 IMPLEMENTATION

The Service can be configured to meet individual organisations' needs. Typically, the following areas may be customised at initial implementation:

- Organisational Structure
- User Access Mechanism
- Workflow
- Theming
- Other Third Party Integration (Crest, CRIS)
- Automated import of content
- Migration from other or different repository platforms

In addition, it can be enhanced with additional features and resources, such as additional storage or the provision of Archive or Off Site Replication services.

The Service Provider will work with the Customer to determine their specific needs and create an implementation scoping document that defines the exact requirements for Implementation. Implementation Charges will be based on this scoping document and are not part of the standard service.

The standard un-customised base Service shall be accessible within twenty (20) Business Days after the applicable Effective Date, the date at which the Service Provider receives the relevant Purchase Order for the Service, provided that the Customer has submitted to the Service Provider any information requested by them. The date upon which the Customer is informed that they can access the service shall be termed the Initial Access Date, regardless of when the Customer actually chooses to access the service for the first time. Service Charges shall start from the Initial Access Date, whether the Customer has submitted the requested information or not.

The full implementation services, specific User Access, Theming, Customisation, Integration, or Migration work that has been purchased as part of a separate Professional Services Agreement shall not be subject to this time limitation. Professional Services work will only be subject to any timeframes in the associated Implementation Agreement.

4 DIGITAL REPOSITORY SOLUTION

The Service provides a Digital Repository embracing the open source community. It is underpinned by Open Source software platforms and plugins which have been selected, refined, and extended by the Service Provider.

The offering will be based on a recent stable release of the core repository software. The Service Provider will regularly review and update this core version as appropriate.

The proper management of digital assets is a vital function of many organisations. The Digital Repository solution provides the following features for your digital assets:

- Flexible access to assets
- Standards-compliant description of assets
- Secure storage of assets

The repository platform is provided pre-configured with plugins that constitute a solution that suit a range of digital assets, these include Publication Repository, Data Repository, Digital Archive, e-Journal, or Special Collections.

The Service Provider regularly reviews the capabilities of their underlying repository solutions and from time to time may make changes to these underlying platforms.

The entire source code of the core Digital Repository Platform is freely available under the GNU General Public License V3. This codebase will be referred to as the Community Platform in this Agreement.

Customisation specific to the customer (for example corporate branding templates, integration with institution authentication systems, or institutional workflows), will not generally be part of the Community Platform and will be managed in separate private code repositories. This code can be provided to the Customer on request under the GNU General Public License V3.

However, customisations that are deemed by The Service Provider to be useful to the community may be included in the Community Platform solely at their discretion.

4.1 RELEASE CYCLE

As part of this Service, the Service Provider will roll out new Releases of the Community Platform to all hosted services at least once per year. The Service Provider solely will determine the content and schedule of these Releases. The Customer shall have no option to refuse or delay the Release. Each Release may include one or more of the following:

- Software version updates (for example, a new core platform release)
- Sustainable Patches backported from later application versions
- Updated plugins
- New plugins
- Removal of plugins
- New features or customisations developed by the Service Provider (for example, as a result of a Request for Customisation)

The Service Provider will provide customers with as much visibility of upcoming releases and their content as is possible. Once released, they will provide customers with release notes detailing all changes made in the new Release.

The Service Provider will provide at least two (2) weeks' notice of the deployment of a new Release. Such deployment may involve up to sixty (60) minutes of Downtime before the new Release is available, although typically this will be undertaken during the Maintenance Window.

4.2 MAJOR PLATFORM OR SERVICE UPGRADE

Sometimes a major core platform or Service change may be planned to take advantage of specific enhanced features or services. Where this is the case, the Service Provider will notify its existing customers at least six (6) months in advance of the expected implementation of this new service/platform. At this stage the Service Provider may alter the service description and pricing for the service and this may also incur migration service fees. At the renewal date, customers can choose to continue based on these principles or terminate their service.

4.3 CRITICAL UPDATES

The Service Provider may, at any time, decide to install a critical update, often for the purpose of improving security or for any other reason. As much notice as possible will be provided but any resulting outage will not be considered a Service Outage.

4.4 MAINTENANCE WINDOW

The Service Provider operates a weekly maintenance window between 7:00am and 9:00am on Tuesday mornings (UK Time Zone only). During this period, the Customer's Service may be either partially or wholly unavailable. The Service Provider will attempt where possible to provide at least five (5) days' notice of maintenance activities that will impact the site. Downtime during this time period shall not be included in Availability calculations (see Monthly Reports).

4.5 PROPOSAL FOR CUSTOMISATION

As well as customisation specific to their own Institution, the Customer may, at any time, propose an addition to the Product Roadmap for the Community Platform which they feel will enhance the Service for all Customers. Customisation may take one or more of the following forms:

- Addition of new or updated Third-Party Plugin
- Addition of Customer-developed Plugin
- Addition of application Patch
- Modification of functionality developed by the Service Provider
- Addition of new functionality proposed to be developed by the Service Provider
- Modification of application Core Code.

The Customer shall record all requests for Customisation via the Service Desk which will also record the status of the request.

The Service Provider will solely determine whether (or not) to incorporate a Customisation request into a future Community Platform update and these would normally be funded by the proposing Customer.

If a request for Customisation is accepted, funded, and approved, it will be made available in a future update and will be provided to all Customers.

4.6 COMMUNITY PLATFORM MAINTENANCE

Unless otherwise agreed by all interested parties, the responsibility to maintain a Community Platform Customisation shall lie with the author of the Customisation, whether that be the Service Provider, the Customer or a third-party. For the purposes of this Agreement, Maintenance will include all code and documentation changes necessary to ensure the Customisation remains suitable for use in the Community Platform. The Service Provider may remove any such Customisation from a future Release if Maintenance is not being appropriately undertaken by the author.

4.6.1 Third Party Applications and Plugins

The Service Provider will report bugs to the application/plugin developers. The application/plugin developers solely will determine whether such bug reports are addressed in future releases of the application/plugin.

4.6.2 Service Provider-Developed Components

Bug Reports for any Service Provider-developed components of the Community Platform will be recorded and the reports made available to Customers. The availability of Bug Fixes for these components will be determined by the Service Provider and may be made available in future updates of the Community Platform. The Service Provider shall solely determine the schedule for such Bug Fixes and may choose to leave a Bug unfixed. Customers can request to assign Support Days to work on a fault in a Service Provider-developed component. Support Days can also be requested to be assigned to investigating customer specific issues.

4.7 COMMUNITY MAILING LIST

Announcements about forthcoming Community Platform changes and releases will be made via the Community Mailing List:

ULCC-RTUG@JISCMAIL.COM

The Customer may provide details of up to three (3) individuals who will be subscribed to the mailing list.

4.8 OWNERSHIP OF INTELLECTUAL PROPERTY

Unless otherwise agreed by all interested parties, the ownership of any intellectual property associated with the Community Platform will lie with the author, whether that be the Service Provider, the Customer or a third-party. Where a Customer submits their developed code for inclusion into the Community Platform, the terms of the GNU General Public License v3 shall apply as this constitutes distribution under the terms of that license.

5 MANAGED HOSTING

The Service Provider provides hosting services for their Digital Repository. The hosting service features and services are detailed in Schedule 6.

Factors such as additional storage requirements, large file sizes (e.g. video files or medical images), or large concurrent usage could all stretch the standard environment's capacity. If an enhanced Virtual Environment is required, this can be purchased as add-on hosting resources.

The base service utilises either Open Source or non-chargeable database infrastructures. Should a Customer prefer to utilise a specific database this would be subject to approval and additional charges.

5.1 RESTRICTIONS ON ACCESS

Customers will not be provided with any access, physical or technological, to the actual infrastructure on which their Digital Repository Service is provided.

5.2 STORAGE

Each service in the customer's Digital Repository portfolio will be given a storage allowance (details in Schedule 6 – Hosting). Any storage used by either the staging or production environments will be deducted from the Storage Allowance.

The customer will be informed of their storage balance at least once per month (see Monthly Reports). As soon as the Storage Balance reaches 100% of the Storage Allowance the Customer will be notified and invoiced for an appropriate increase in Storage Allowance. If after fourteen (14) days, the Storage Balance still exceeds 100% and the Customer has not provided a PO matching the supplied invoice then the Service Provider will no longer guarantee any of the service levels defined in this Agreement.

The Customer can increase their Storage Allowance by contacting the Service Desk. Additional storage will be provided within five (5) Business Days of the Service Provider receiving the Customer's Purchase Order. The minimum period that additional storage can be provided for is twelve (12) months or prorated until the next contract renewal date.

5.3 BACKUP

As part of the service, data associated with the Customer's instance of the Digital Repository Service will be backed up according to the terms of the Schedule 6 - Hosting. Summarised here as:

Frequency	Policy	Target Device	Retention
Daily	Incremental	Disk (onsite)	7 days
Weekly	Full	Disk (onsite)	21 days
Weekly	Full	Tape (offsite)	21 days

Service Backups are primarily for disaster recovery purposes.

Any Customer requests to access/restore this data should be processed as a Customisation request Support Case.

5.4 ARCHIVAL STORAGE

The Service Provider can provide additional archival services whereby data is archived for long term accessibility across multiple storage locations. The setup and use of this facility is not part of the base service but can be purchased as a separate option.

5.5 OFF-SITE REPLICATION

The Service Provider can provide an Off-site Replication Service (Described in Schedule 7) whereby the repository site is replicated. The setup and use of this facility is not part of the base service but can be purchased as a separate option.

6 SUPPORT SERVICES

The Customer will be provided with access to the Service Provider's Service Desk which can be used to log new Support Cases and track progress of open Support Cases.

6.1 SUPPORT HOURS

Support hours are 08:30 to 17:30 (UK Time Zone only), excluding weekends, Statutory Holidays and University of London Closure Days (see the University of London website for full details).

6.2 CONTACT DETAILS

The Customer can contact the Service Desk using any of the following channels:

Online	https://ulcc.service-now.com	Log new Support Case or track progress of open Support Case	Any time
Email	service@london.ac.uk	Log new Support Case	Any time
Telephone	020 7862 8111	Log new Support Case	During Support Hours

6.3 ESCALATION

If for any reason the Customer is not satisfied with the response provided by the Service Desk, Support Cases can be escalated as follows:

1st Level Escalation	Digital Repository Team Service Manager	drtservicemanager@ulcc.ac.uk
2nd Level Escalation	Head of Software Services	headofsoftwareservices@ulcc.ac.uk

6.4 SUPPORT CLASSIFICATION

The Research Technologies team can provide a broad range of expertise for the Customer to draw on to ensure the successful operation of their Service.

When logging a Support Case the case will be classified depending on the type of issue

- Hosting Platform Issue – Service failure due to issue with the hosting environment
- Current Service Incident – Issue regarding the platform application (i.e. non-hosting based problem)
- Advice / Consultancy
- Customisation or Request for Change

Hosting Platform Issues are caused by a failure of service due to a problem with the hosting infrastructure, such as server or network switching failure. The Service Provider have a dedicated infrastructure team that manage their hosting environments and are well versed in ensuring reliable and performant hosting services. Time spent on resolving these incidents by the Service Provider is fully inclusive within the service provision.

A Current Service Incident is used to classify other service issues that are not due to the hosting environment. The Service Provider's technical teams provide support services for a wide range of leading digital repositories and as such are experienced in assisting customers to obtain a timely and effective outcome to any incident. The Service provides an initial allowance for Support Days.

Advice and Consultation services enable the Customer to get the best experience from their Service. The Service Provider has a long history of expertise in digital and institutional repositories and can readily assist their customers with feedback and assistance based on many years of experience.

Time allocated to this work can be typically used to discuss best practice, the operation of specific features, working practices, or determine the scope for future Customisation Requests. The Service provides an initial allowance for Consultancy Days.

A Customisation Request will be handled by the Professional Services team and any work undertaken is not part of the standard service described in this Agreement but can be purchased and supplied alongside the Digital Repository service described herein. All customisation and development activities should be logged under this category. Consultancy Days can be used prior to ordering Professional Services to discuss suitability, scoping and estimating.

Professional Services offered include:

- Customisation and development
- Integration with Customer systems and infrastructure
- Migration from existing repository systems
- Branding

6.5 SUPPORT AND CONSULTANCY ALLOWANCE

The service includes a Support and Consultancy Allowance of included days per annum.

As Current Service Incidents and Advice Support Cases are worked, the time taken will be deducted from the current Support and Consultancy Balances.

For the purposes of calculating the Support and Consultancy Balance, a day is defined as seven (7) hours. At the end of each 12-month period, on renewal the Support and the Consultancy Balances will be reset to the annual figure. There is no ‘rollover’ of balances to subsequent years. If the contractual period is less than twelve (12) months, the Support Allowance will be allocated on a pro-rata basis (to the nearest hour).

Customers may purchase additional Support+ service which increases the allowance provided.

6.6 INCLUSIVE ACTIVITIES

The following support activities will not result in any alteration of the Customer's Support or Consultancy Balance:

- Hosting Platform issue resolution, except where subsequently attributed to external Customer system(s) or non-compliance with Acceptable Usage Policy.
- Maintenance of the Digital Repository associated infrastructure (including security patching and deployment of software updates).

6.7 BALANCE USING SUPPORT CASES

All other Support Cases will result in a deduction from the Customer's Support or Consultancy Balance or be delivered if approved under a separate Professional Services Agreement.

6.8 BALANCE CALCULATION

Any Balance qualifying work on the Support Case will be rounded up to a minimum of 15 minutes for each interaction. After 15 minutes of continuous activity has elapsed the actual time expended will be allocated to that Support Case for that interaction.

6.9 BALANCE REPORTING

The Customer will be informed of their Support and Consultancy Balance at least once per month (see Monthly Reports). The Customer will be informed within one (1) Business Day of the original Support or Consultancy Allowance being used up.

It either Balance is exceeded the Customer will need to top up their allowance within ten (10) Business Days of notification. The Service Provider reserves the right to withhold the handling of any Support Cases until the Balance is returned to credit.

7 SERVICE MANAGEMENT AND REPORTING

The Service Provider will provide (via e-mail) the Customer with one report per calendar month. That report will include the following information for the previous month:

Support and Consultancy Balance Used
Support and Consultancy Balance Remaining
Support Cases Summary
Storage Usage
Availability level achieved
Number of Service Outages
Service Outage Summary

The Customer acknowledges and agrees that any of the foregoing reports will constitute Confidential Information for the purposes of this Agreement.

In addition to the monthly reports, as part of the Service the Service Provider will hold a formal Service Review during the term of the annual service to share feedback on the service.

8 SERVICE LEVELS

8.1 SERVICE CREDITS

The Customer agrees that the service credits referred to in this Agreement shall be the Customer's sole remedy, and the Service Provider's sole obligation, with respect to failures of the Digital Repository Service to meet the service levels defined by this Agreement. Service credits shall be applied to the fees for the affected Digital Repository Service for the subsequent period. In order to receive any service credit, the Customer must notify the Service Provider within thirty (30) days from the time Customer becomes eligible to receive a service credit. Failure to comply with this requirement will forfeit the Customer's right to receive a service credit. In order to be eligible, the Customer must be in compliance with the Agreement including the Reasonable Usage Policy. The maximum number of service credits to be issued by the Service Provider to the Customer during any given calendar month shall not exceed the fees paid by Customer for the affected Digital Repository Service(s) for such month.

8.2 AVAILABILITY AND PERFORMANCE

The Digital Repository Service will be accessible twenty-four (24) hours a day, seven (7) days a week, with a 99.9% targeted uptime. 99.9% uptime means that for 99.9% of the time during any calendar month, the Digital Repository Service will be available. Unavailability is a condition in which the Digital Repository Service's Primary URL cannot be accessed from a UK location. Each instance of unavailability is a Service Outage.

Where the Primary URL does not return with the expected page within thirty (30) seconds, this shall be considered to be the start of a Service Outage.

Where the load time of the Primary URL is greater than five (5) seconds for five (5) consecutive measurements, this will be recorded as the start of a Service Outage. The outage will continue until

the load time returns to less than five (5) seconds. The Outage Period begins at the end of the triggering period of five measurements. This triggering period is not included in the outage duration.

The availability of the service will be checked by the Service Provider at least once per minute from an external UK location. If such a Service Outage occurs, they will notify the Customer's Service Outage Notification Contact via email. This notice will include the reason for the Service Outage and the estimated time for restoration of the Digital Repository Service if the Service Provider knows this information when it gives this notice. The Service Provider will also notify the Customer's Service Outage Notification Contact via e-mail once the Service Outage is over and the Digital Repository Service is restored.

Following recovery from any particular Service Outage, the Service Provider will provide the Customer with a post-incident summary that will include:

- Cause of the Service Outage (if determined)
- Method used to correct the problem
- Measures the Service Provider will take to prevent similar Service Outages in the future (if any)
- Which service credit exclusions apply (if any)

Whilst Overall Availability will be the availability of the service measured 24/7/365, calculation of availability for the purpose of service credits (Contractual Availability) shall be based on availability during Business Hours only (8:30-17:30 Mon-Fri, Statutory Holidays excluded).

99.9% **Overall Availability** means that the Digital Repository Service is unavailable for no more than forty-three (43) minutes (based on a 30-day month). Calculated as follows:

$$\frac{(Total\ number\ of\ minutes\ in\ month - Total\ duration\ of\ all\ Service\ Outages)}{Total\ number\ of\ minutes\ in\ month\ x\ 100}$$

99.9% **Contractual Availability** means that the Digital Repository Service is unavailable during Business Hours for no more than sixteen (16) minutes (based on a 30-day month). Calculated as follows:

$$\frac{(Total\ number\ of\ Business\ Minutes\ in\ month - Total\ duration\ of\ all\ \boldsymbol{Qualifying}\ Service\ Outages)}{Total\ number\ of\ Business\ Minutes\ in\ month\ x\ 100}$$

If Contractual Availability is less than 99.9% in a given month then 5% of the following month's Digital Repository Service fees will be credited.

All Service Outages shall qualify for inclusion in the Contractual Availability calculation unless they are attributed by the Service Provider to one or more of the following.

- Downtime taking place outside of Business Hours
- Downtime requested by customer
- Downtime resulting from Customer not complying with Reasonable Usage Policy
- Downtime resulting from services, hardware, or software provided by the Customer or a third party
- Downtime resulting from installation of code that is not part of the latest Community Platform Release
- Outages taking place due to any form of DNS redirect that is not the responsibility of the Service Provider
- Downtime taking place during Maintenance Window
- Downtime caused by the Customer's use of the Service after the Service Provider's advice to modify use of the Service, if the Customer did not modify use as advised

- Downtime resulting from unauthorized action or inaction or from the Customer's employees, students, agents, contractors, or vendors, or anyone gaining access to our network by means of your passwords or equipment
- Downtime due to factors outside the Service Provider's control (for example, natural disaster, war, acts of terrorism, riots, or government action)
- Material changes to the institution or the intended service usage such that a different service would have been proposed by the Service Provider

Customers are entitled to monitor availability of their service via external means but any such measurements shall not result in any obligation on the Service Provider to deliver service credits.

Where the Customer plans to make changes to their systems that may impact availability of the Digital Repository Service, the Customer is required to provide at least five (5) Business Days' notice to the Service Provider. Failure to provide such notice may result in charges being levied for the time taken by the Service Provider's staff to respond to and investigate the resulting outage. Any such charges will be levied at the standard Day Rate in operation at the time.

Please refer to the Service Provider's Enhanced Availability service for the option to use Overall Availability measurements as Contractual Availability.

8.3 HOSTING PLATFORM ISSUE RESOLUTION

The Service Provider classifies Support Cases as Incidents according to the following ITIL and ISO2000 definitions:

An unplanned interruption to an IT Service or a reduction in the Quality of an IT Service. (ITIL v3)
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. (ISO2000)

Both of these definitions exclude Bugs, whether in the Service Provider's code, application code or third-party code.

These incidents are further classified by the Service Provider as Hosting Platform Incidents where they relate to the Hosting Infrastructure.

The following resolution service levels apply to Hosting Platform Incidents only.

Priority	Definition	Resolution Time	Scenarios
P1	Showstopper, significant business or user impact	4 Business Hours	• Service (as identified by Primary URL) is unavailable • Sensitive data (e.g. user account information) has started to be exposed • Service has degraded in such a way as to prevent substantially all users (> 75%) from accessing all or most data or screens. • Data has become corrupted
P2	High priority, impacting effective use of the service for a significant number of users	1 Business Day	• One or more plugins have become completely unavailable. • Service has become unavailable to at least 25% of user population. • Service has degraded in such a way as to prevent a significant number of users (>25%) from accessing all or most data or screens.

			• Service performance (against service level) has degraded significantly. • Submission of data and/or files is no longer possible
P3	Normal priority, service impaired for a small number of users	4 Business Days	• Anything not covered by P1,2, or 4
P4	Low priority, service not functioning as expected, but not significantly affecting use	10 Business Days	• Service has degraded but impact is purely aesthetic • Service has degraded such that functionality is affected but a workaround is possible.

The Service Provider is unable to provide any commitment to Resolution Time for Incidents resulting from:

- Other Support Case Types
- Customer not complying with Reasonable Usage Policy
- Failure of external (non-Service Provider controlled) system or network (e.g. Customer's Active Directory or JANET)

9 CUSTOMER RESPONSIBILITIES

9.1 MANAGEMENT AND USE OF SERVICES

Excluding the configuration details that allow the Digital Repository Service to operate, the Service Provider is not responsible for management and actual use of the features and functions of the Service.

Although the Service Provider's support team can offer information, advice and assistance, the Customer bears all responsibility for the remaining management and actual use, including, without limitation:

Customer Responsibilities	ULCC Responsibilities
Creating/Removing Active Users	Enabling/Disabling Plugin(s)
Modifying all Active User Information	Altering Administration setting(s)
Managing Security of User Accounts	Altering Configuration setting(s)
Creating/Removing records (publications, archive entries, e-journals, etc.)	
Modifying records	
Bulk Editing records	

9.2 RESPONSE TO REQUEST FOR ACCEPTANCE OR ADDITIONAL INFORMATION

In order for the Service Provider to effectively operate this Service, it is important that The Customer confirms acceptance of all delivered customisations, fixes or enhancements in the staging/UAT environment.

The Service Provider will notify the Customer whenever items are ready for acceptance.

Likewise, if an incident has been raised, the Service Provider may need additional information from the Customer to progress this. The Service Provider will notify the Customer if more information is required.

The Customer must respond in a timely manner to enable the Service Provider to proceed with these items. If a response is not received within ten (10) Business days of the notification, then the item will be assumed to be accepted or the incident no longer valid. If relating to a change the Service Provider will take this as authority to propagate the relevant changes to the production server and in any case close the relevant incident or change item.

9.3 SERVICE URL

The Digital Repository Service will be a ulcc.ac.uk URL.

Registration and management of additional Service URLs and Certificates (e.g. http://research.university.ac.uk) is the responsibility of the Customer.

9.4 ACCEPTABLE USAGE POLICY

The Customer agrees to comply with the Reasonable Usage Policy outlined in

Appendix B: Acceptable Usage Policy.

9.5 NOMINATED CONTACTS

Only Registered Users may submit Support Cases to the Service Desk online and via email.

The Customer agrees to nominate at least one (1) individual who will be registered for Service Desk access. The Service Provider cannot action Support Cases logged by unregistered users, so the Customer also agrees to notify the Service Provider of any changes to the list of nominated individuals in order that these changes can be reflected in Service Desk.

Confirmation of currently held list of nominated contacts will be a condition of service renewal.

9.6 RESTRICTIONS ON ACCESS

Customers will not be provided with any access, physical or technological, to the infrastructure on which their Digital Repository Service is provided.

10 TERMINATION OF SERVICE

10.1 NOTIFICATION

Subject to the notice period outlined in The Service Provider's standard Terms and Conditions and any other legal agreement made between the parties, the Customer may notify the Service Provider of its intention to terminate its use of the Digital Repository Service. The Customer shall provide to the Service Provider the final date on which they will use the service. The next Business Day after this will be termed the Termination Date. The Service Provider will acknowledge this notification within five (5) Business Days.

10.2 ACCESS TO SERVICE

Customer access to the Digital Repository Service will be removed at any time on or after the Termination Date. No response shall be provided to Support Cases on or after the Termination Date.

10.3 EXIT SERVICES

A Customer can request Exit Services from the Service Provider on Termination of the Service.

The scope and charge for these services is not included within the Service and needs to be agreed separately as part of a Professional Services Agreement.

However, subject to the purchase of the specific Exit Service the Service Provider can typically provide, to the Customer:

- The entire source code of their Digital Repository Service at the time of termination
- All Customer content stored within the Digital Repository Service
- A Redacted Database dump where "Redacted" means the removal of any confidential data such as passwords.

11 APPENDIX A: DEFINITIONS

Active Directory	Active Directory (AD) is a directory service that Microsoft developed for Windows domain networks and is included in most Windows Server operating systems as a set of processes and services.
Agreement	This document, once signed or otherwise accepted by both parties.
Bug Fixes	A correction to a bug in the Digital Repository software
Business Days	Mon-Fri, statutory holidays excluded
Business Hours	08:30-17:30 Mon-Fri, statutory holidays excluded
Consultancy Allowance	The total amount of consultancy time available to the Customer in a given year of service
Consultancy Balance	The remaining amount of consultancy time available to the Customer in the current year of service (Consultancy Allowance – Time Used To Date)
Confidential Information	Information relating to the Service Provider that is shared with the Customer that must not be shared with other individuals/organisations.
Contractual Availability	The availability of the Digital Repository Service throughout a one month period during Business hours, unless accompanied by a subscription to an Enhanced Availability, Enhanced Availability+ or OOH Call Centre service.
Customer	The organisation that is paying for the service described by this document.
Customisation	Referring to alteration of the underlying Digital Repository software code by any means.
Designated Contact	A single individual that the Customer designates as responsible for their subscription to the Digital Repository Service.
Digital Repository Service	The service described by this Agreement
Digital Repository Software	The software to which the Customer is provided access upon subscribing to the Digital Repository service. The software comprises the core application platform plus extensions and modifications selected by the Service Provider.
Effective Date	The date upon which the contract containing this Agreement formally begins.
Initial Access Date	The date upon which the Customer is able to access the service and the date from which the charges will begin accumulating.
Maintenance Window	A period of time which is reserved for regular planned maintenance of a Service. During time the Customer is aware that the Service might be impacted.
Outage Period	The period of time covered by a specific Service Outage.

Overall Availability	The availability of the Digital Repository Service throughout a one month period including both Business and non-Business Hours.
Primary URL	Primary URL shall be the address normally provided to users as the access point to the Customer's Digital Repository service, e.g. eprints.institution.ac.uk.
Reasonable Usage Policy	A supporting document to the Digital Repository SLA outlining actions or activities which are considered to be outside of the purpose of the service, or which make the service particularly onerous to provide.
Redacted Database	A copy of the complete database used by the Customer's Digital Repository Service with security-related information removed such as the Service Provider's administration passwords, connection details etc.
Release Date	Date of release for software, plugins, patches, bug fixes
Resolution Time	The elapsed period of time between the Service Provider being made aware of an Incident and service being restored to its pre-incident state.
Service Charges	Charges paid by the Customer for receipt of the service described in this document.
Service Credits	Service credits are the mechanism by which future payments are reduced if the Service Provider's performance fails to meet the performance standards set in the service levels set out in this document.
Service Outage	A specific period for which the service was unavailable.
Service Outage Notification Contact	A single individual (or e-mail) that the Customer designates as requiring to be notified during any Service Outage.
Service Provider	The organisation providing the services described in this contract.
Service Requests	Customer requests for services related to the Digital Repository software
Storage Allowance	The total amount of disk storage available for Customer e-Learning content.
Support Allowance	The total amount of support time available to the Customer in a given year of service
Support Balance	The remaining amount of support time available to the Customer in the current year of service (Support Allowance – Time Used To Date)
Support Case	A single set of interactions between the Customer and the Service Provider covering a single incident or request.
Support Portal	Software operated by the Service Provider's Support team that enables incidents/requests to be logged via the web.
Termination date	The Customer shall provide to the Service Provider the final date on which they will use the service. The next Business Day after this will be termed the Termination Date

Third Party Code	Code which is provided by an individual or organisation other than the core application platform provider, the Service Provider or the Customer
Third Party Plugin	A Plugin to the Digital Repository Software which is not included in the base build and developed by a third party.
Unavailability	Unavailability is a condition in which the Digital Repository Service's Primary URL cannot be accessed from a UK location

12 APPENDIX B: ACCEPTABLE USAGE POLICY

The following actions or events committed by the Customer or those that it is responsible for shall be deemed to be contraventions of the Acceptable Usage policy:

1. Denial of Service (DoS) attacks
2. Any action which prevents the Service Provider accessing its administrator accounts
3. Ignoring of written Service Provider's advice to modify use of the service(s) provided in cases where the Customer's use of the service(s) causes a Service Outage
4. Excessive e-journals on a single e-Journal Management service

Furthermore, any abuse of the acceptable use policy of the JANET network (currently available at: http://www.ja.net/services/publications/policy/aup.html) will be regarded as unacceptable use of the Repository Technologies Service.

SCHEDULE 3

DIGITAL REPOSITORY – DATA PROTECTION

1. Data Protection

1.1. In this Schedule 'the Act' means the Data Protection Act 1998 together with the Regulations made pursuant to that Act and/or any superseding legislation.

1.2. Each Party shall comply at all times with the Act in respect of any Personal Data processed by it pursuant to this Agreement.

1.3. In respect of any Personal Data processed by either Party pursuant to this Agreement, each Party warrants to the other that it has made all necessary notifications to the Information Commissioner, in accordance with the Act.

1.4. The Customer shall be the Data Controller of all Personal Data for the purposes of this Agreement and shall solely determine the purposes for which and the manner in which the Personal Data are processed by providing the Service Provider with express written instructions (whether in the form of specific instructions or through an operations manual setting out permitted processing of Personal Data, or by way of this agreement) as to the processing of Personal Data that may be carried out by the Service Provider or on the Service Provider's behalf through a third party under a Third Party Data Agreement.

1.5. The Service Provider agrees

1.5.1. to put in place arrangements and to process Personal Data received or obtained from or on behalf of the Customer in a manner to enable the Customer to comply with the Act.

1.5.2. The Service Provider as Data Processor agrees:

a) to ensure that appropriate technical and organisational measures are adopted by it to ensure safekeeping against unauthorised or unlawful processing of the Personal Data and against accidental loss, or destruction of, or damage to the Personal Data, as required by the Act;

b) to use the Personal Data solely for the purpose of performing its obligations under this Agreement;

c) to process the Personal Data only as a Data Processor in accordance with the instructions of the Customer,

d) to provide promptly to the Customer from time to time as part of this Agreement such information and access as the Customer may require in relation to the Personal Data;

e) to direct data protection enquiries from Data Subjects to the Customer's data protection officer (as notified by the Customer to the Service Provider from time to time) and to promptly forward all subject access requests to the Customer's data protection officer promptly and in any event within 5 Business Days from receipt;

f) not to transfer any of the Personal Data to a country outside the European Economic Area other than as provided by clauses 3.1 and 3.2 of this schedule;

g) to make arrangements to ensure that back-up records of the current Personal Data are maintained and updated on a regular basis;

h) to have appropriate procedures in place for the archiving and eventual destruction of Personal Data, subject to the agreement of the CUSTOMER; and

i) to ensure that any employee, or Subcontractor engaged by the Service Provider receives adequate training to ensure compliance with this Clause.

Should the Service Provider no longer need any of the Personal Data for the performance of the Services it shall return that Personal Data (and any copies of it) to the Customer in hard copy or in electronic form or at the request of the Customer shall destroy the Personal Data.

2. Third Party Data Processors

2.1. Before appointing any third party Data Processor, the Service Provider shall request the written approval of the Customer and shall provide all details that the Customer may reasonably require to determine whether the third party should act as a Data Processor pursuant to this Agreement.

2.2. The Service Provider shall seek the express authorisation of the Customer for any processing of Personal Data by a third party Data Processor and shall ensure that the third party Data Processor acts at all times as a Data Processor of the Personal Data.

2.3. The Service Provider shall ensure that each agreement between it and a third party for the processing of any Personal Data under this Agreement (**"Third Party Data Agreement"**) is no less restrictive and protective of that Personal Data than the provisions of Clause 1 of this schedule. In particular, the Service Provider shall ensure that each Third Party Data Agreement includes provisions:

a) that allow the Customer to enforce rights directly as against the third party Data Processor as a beneficiary under the Contracts (Rights of Third Parties) Act 1999;

b) that the third party shall act only as a Data Processor for the Customer under the Agreement; and

c) that the third party shall not undertake any processing other than in accordance with the written instructions of the Customer under Clause 1.4 of this schedule.

2.4. The Service Provider shall submit a draft of each proposed Third Party Data Agreement to the Customer for approval before entering into it. The Customer shall have the right to make any recommendations for amendment of that Third Party Data Agreement that it considers necessary or desirable. The Customer shall have the right to withhold approval to any Third Party Data Agreement in its absolute discretion.

2.5. The Service Provider shall procure compliance of the third party Data Processor with all of its obligations under the Third Party Data Agreement

3. International Data Transfers

3.1. The Service Provider shall not transfer, and shall not enter into any arrangement for the transfer, of any Personal Data under this Agreement outside the European Economic Area without the express approval in writing of the Customer.

3.2. If the Customer so requires, the Service Provider shall enter into a data transfer agreement with the Customer (or shall procure that the relevant third party enters into a data transfer agreement with the Customer) which as a minimum, shall reflect the

model Clauses approved by the European Commission under Commission Decision 2002/16/EC16.

SCHEDULE 4

DIGITAL REPOSITORY – FREEDOM OF INFORMATION

1. General

1.1. Each of the Parties acknowledges that the other Party is subject to the requirements of the Freedom of Information Act 2000 (in this Schedule 4 referred to as 'the Act') and the Environmental Information Regulations and shall assist and cooperate with the other Party to enable it to comply with its Information disclosure obligations.

1.2. Each party shall, and shall procure that any sub-contractors shall, transfer to the other Party all Requests for Information that it receives as soon as practicable and in any event within 5 Working Days of receiving a Request for Information;

1.2.1. Provide the other Party with a copy of all Information in its possession or power in the form that the other Party requires within 5 Working Days (or such other period as the other Party may specify) of the other Party's request; and

1.2.2. Provide all necessary assistance as reasonably requested by the other Party to enable the other Party to respond to the Request for Information within the time for compliance set out in section 10 of the Act or Regulation 5 of the Environmental Information Regulations.

1.3. The Party to which the Request for Information is addressed shall be responsible for determining in its absolute discretion and notwithstanding any other provision in this Agreement or any other agreement whether the Commercially Sensitive Information and/or any other Information is exempt from disclosure in accordance with the provisions of the Act or the Environmental Information Regulations.

1.4. Each Party acknowledges that the other Party may, acting in accordance with the Secretary of State for Constitutional Affairs Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Act ("the Code"), be obliged under the Act or the Environmental Information Regulations to disclose information concerning the Parties or the Services in certain circumstances:

a) without consulting the other Party; or
b) following consultation with the other Party and having taken its views into account;

provided always that the Party to which the Request for Information is addressed shall, in accordance with any recommendations of the Code, take reasonable steps, where appropriate, to give the other Party advanced notice, or failing that, to draw the disclosure to the other Party's attention after any such disclosure.

1.5. Each party shall ensure that all Information is retained for disclosure and shall permit the other Party to inspect such records as requested from time to time.

1.6. Each party acknowledges that the Commercially Sensitive Information (all pricing information and all personnel information, specific technical details describing solutions and/or functionality) is of indicative value only and that it may be obliged to disclose it in accordance with the Act and the provisions of this Schedule 4.

SCHEDULE 5

DIGITAL REPOSITORY – CONFIDENTIALITY

1. General

1.1. Subject always to schedule 4, each Party ("Recipient") undertakes to treat as confidential all Confidential Information of the other Party ("Disclosing Party").

1.2. The Recipient may only use the Confidential Information for the purposes of this Agreement and may provide its employees, directors, subcontractors, agents, third party suppliers and professional advisers ("Permitted Users") with access to the Confidential Information only to the extent required for the performance of this Agreement or the receipt of the Services. The Recipient shall ensure that each of its Permitted Users is bound to hold all Confidential Information in confidence to the standard required under this Agreement and complies with such obligations of confidence.

1.3. This Schedule 5 shall not apply to any information which:

1.3.1. enters the public domain other than as a result of a breach of the provisions of this Schedule 5;

1.3.2. is received from a third party which is not known (and ought not to be known) to the Recipient to be under a confidentiality obligation in respect of that information;

1.3.3. is independently developed by the Recipient without use of the Disclosing Party's Confidential Information; or

1.3.4. was lawfully in the possession of the Recipient prior to disclosure (as evidenced by the records of the Recipient).

1.4. The Recipient may disclose Confidential Information where required to do so by any law or by the order of any court or other authority with the right to compel disclosure. In these circumstances, the Recipient shall give the Disclosing Party prompt advance written notice of the disclosure (where it is lawful and practical to do so) so that the Disclosing Party has sufficient opportunity (where possible) to prevent or control the manner of disclosure by appropriate legal means.

SCHEDULE 6

DIGITAL REPOSITORY MANAGED HOSTING SERVICE LEVEL AGREEMENT

1. Introduction

1.1. This schedule provides a definition of the DART Managed Hosting services and service levels provided by The Service Provider.

1.2. The Service are housed in the Service Provider's Data Centre (The Facility).

2. The Service Provider's Data Centre

2.1. This Facility has been designed to the following specification and the Service Provider will use reasonable endeavours to maintain the Facility to these design specifications.

2.2. For the Facility's air-conditioning design:

2.2.1. The air-conditioning units, with built-in resilience and under floor cooling, maintain room temperature at 24 degrees C ± 2 degrees C and humidity at 50% ± 5%, with a cooling load per rack of 1.5kw. The air conditioning units have been provisioned to support an environment assuming maximum rack and power utilisation across the whole Facility.

2.2.2. The resiliency allows the suite to be maintained by eight out of the ten air conditioning units to cover against full or partial failure of a unit without detriment to the service.

2.2.3. The Service Provider will use reasonable endeavours to ensure that the air conditioning maintains the air temperature and humidity within the levels specified in this section.

2.3. For the Facility's Electricity Supply:

2.3.1. Each Rack position has two power strips fed from diverse distribution boards (A&B) operating at AC240V, with 32 amp breakers to BS4343 (blue commando type) sockets underneath each rack position. The average power usage per rack cannot exceed 6 Amps to allow full N+1 UPS resiliency.

2.3.2. The UPS is designed to generate an output at 240 volts + or - 50 Hz. UPS equipment maintenance is required to be performed every twelve (12) months, and battery maintenance every six (6) months, each maintenance session will last no longer than four (4) hours.

2.3.3. A second power feed is obtained from Senate House (the building adjoining the data centre location) and is fed from a different transformer. In the event of a failure of the primary feed, automatic switching will transfer the load across to the secondary feed, with the data centre load being supported by the UPS units. In the event that mains power is not available on the second feed as well, the standby generator shall start.

2.3.4. The onsite standby generator of 900kVA will provide standby power to the data centre and associated plant equipment, with a remote fuel tank to provide up to 24 hours of continuous running.

3. Services

3.1. For the purposes of these terms and conditions, "Business Day" means Monday to Friday, excluding any bank holidays within England and "Business Hours" means 8.30am to 5.30pm on a Business Day;

3.2. For Data Centre Environmental Services the Service Provider will use reasonable endeavours to:

3.2.1. Notify the Customer during Business Hours, or where outside Business Hours at the start of the next Business Day, within 30 minutes, of:

- Any Security Incident affecting the Facility;
- Any fire or flood condition within the Facility (except false alarm);
- Any complete air conditioning failure or out of specification environmental condition longer than 2 hours;
- Data Centre running under generator power due to major power failure;
- Loss of network functionality

3.2.2. Provide access to other services required within an agreed timetable (note that third party network connection usually has a third-party installation lead-time of 90 Business days).

3.2.3. Maintain full fire protection for the room utilising Argonite fire suppressant, a fully automatic, gas release system and a VESDA system for the detection of smoke particles.

3.2.4. Provide resilient power to each Rack fed from separate PDUs, connecting each PDU to its own UPS unit with a listed autonomy of 30 minutes at N full UPS load.

3.2.5. Provide dual power feeds to the UPS from separate transformers.

3.2.6. Provide flood detection.

3.2.7. Provide CCTV and secure access doors to the main suite, lobby, and corridors.

3.2.8. Provide manned security 24x7x365.

3.2.9. Provide access to the JANET Network for authorised customers. This link is 2 x 10Gbps.

3.2.10. Provide access to a 3rd party commercial network for Internet access, if that is part of the contracted Service, for those Customers unable to use the JANET network.

3.2.11. Provide second diverse data communication network routes if required, via a 3rd party commercial network, if that is part of the contracted Service.

3.2.12. Perform such general janitorial services, environmental systems maintenance, power plant maintenance and other actions as are reasonably required to

maintain the Facility in good condition and suitable for the purposes defined above.

3.2.13. Monitor all Services on a 24/7 basis via alarm reporting systems to enable timely remedial action where they are in jeopardy or malfunctioning. Monitored conditions are Fire, Flood, Temperature, Humidity and Power.

3.2.14. Provide two weeks' notice of any planned work to the features of the Facility outlined above, except where the work is in extremis where as much notice as is reasonably possible of the expected outage will be given ahead of time.

3.2.15. Ensure that any planned work that has a risk of affecting the technical and operational conditions of the Facility is restricted to Tuesday morning periods between 07:00 and 09:00 where possible,

3.2.16. Ensure that all other work is carried out between 00:00 and 05:00 where possible.

4. General Hosting Services

4.1. The Service Provider will use reasonable endeavours to ensure that Managed Services meet the following criteria:

4.1.1. All Service Provider's hardware that is utilised for the Services will be subject to a current maintenance contract with a reputable supplier with a response time of 4 hours.

4.1.2. All Service Provider's hardware that is utilised for the Services is replaced at the end of its normal operating life.

4.1.3. For Service Provider's hardware the network connections to and within the Facility will be protected by network security systems integrating firewall, Denial of Service (DoS) protection, virtual private network (VPN) and traffic management functionality so as to protect all Services hosted at the Service Provider from external network attack.

4.1.4. For non-Service Provider hardware the agreed level of security will be provided.

4.1.5. The operating systems of all equipment required to deliver the Services are maintained at the appropriate patch and release levels.

4.1.6. Applications are installed or upgraded in line with the requirements of the Services, however, any software upgrade that is found to be to the detriment of other Services being supplied will not be applied.

4.1.7. Upgrades of software or hardware affecting a single Customer will be scheduled at times agreed with the Customer.

4.1.8. Equipment required to deliver the Services will be individually connected to the Facility network at a minimum of 100Mbps.

4.1.9. Data Storage required to deliver the Services will utilise RAID technology to spread data across a number of discs with redundancy so that if any individual disc fails, data is preserved and access can continue.

4.1.10. Where it is part of the Contracted Service, Customer data will be backed up to tape on a regular basis, with full backups being taken weekly and incremental

backups taken daily. These backups are intended for the purpose of restoring the data in the unlikely event of a system failure and are not intended for long term preservation. The restoration of individual files is not part of this service.

4.2. For the avoidance of doubt the Service Provider is not responsible for:

4.2.1. Hardware, software or applications that are installed and managed by third parties.

4.2.2. Software incompatibilities arising from the installation of new releases of Third Party software (including Open Source Software).

5. Digital Repository Managed Hosting Environment

The following sections describe the Digital Repositories' specific hosting environment provided as part of this service.

5.1. Firewall

5.1.1. Multiple levels of security are employed to protect the services. The firewall utilises policies to permit or deny access to resources. These are granular to the service port and IP address level. A software firewall is additionally installed on the server to provide further protection at the network level.

5.1.2. Other tools are utilised to monitor, report and alert on targeted attacks against services. This utilises a signature based solution to review all packets traversing the network.

5.2. Site Certificates and Naming

5.2.1. All sites will be deployed for https access and not http.

5.2.2. A UoL site name will be deployed unless a different name is specified by the Customer. Where a non UoL site name is deployed, the Customer will be responsible for providing and maintaining the certificate.

5.3. Virtual Server Allocation

5.3.1. A separate VM is assigned for each Live instance of the repository. The standard Service provides the following allocation of resources to the Live VM.

CPU	RAM	System Disk
Equivalent 2.2GHz	4 GB	50GB

5.3.2. Other resources options are available if required, but will be at additional cost.

5.4. Virtual Server Environment

5.4.1. The servers are configured as a VMWare High Availability environment providing server failover as part of this infrastructure. The standard build currently includes the agreed versions of

- VMWare
- LAMP Stack of
  - Red Hat
  - Apache
  - MySQL

    - Perl/PHP
- Digital Repository Application
- Backup client

5.5. UAT / Staging Environment

5.5.1. A UAT / Staging environment is required for the Customer to sign off changes or upgrades. This can also be used for the Customer to review system behaviour or for training purposes.

5.5.2. It is necessary for the Customer to either purchase a full replication of the Live environment for their sole use or else purchase the provision of temporary access to a more generic platform.

5.5.3. The Full UAT / Staging environment where purchased will be configured as per the Live Environment and be available to the customer as required.

5.5.4. Where a temporary UAT/Staging environment is purchased this can be made available for a maximum of 25 day's in total. The Service Provider will notify the Customer when the environment has been provisioned to sign off changes or upgrades. The Customer should give at least 5 Business Days' Notice for any requirements to access this environment for their own purposes. The Service Provider will provide the environment and notify the Customer of the access details as per the required access date or 5 Business Days after notification if sufficient notice has not been given.

5.5.5. This temporary environment will be based on the standard generic platform build and populated with the customer's configuration. The environment will not standardly contain the Customer's data but may be loaded with some test data where appropriate.

5.5.6. In order to allow flexibility of how these 25 days are used (either as a continuous block or multiple instances), setup and deactivation effort will be taken from the Support Days Allowance and will need to be in credit to cover this activity.

5.5.7. Additional requirements and/or usage of the temporary environment can be purchased as additional services.

5.6. Load Balancing

5.6.1. The standard configuration does not include load balancing but this can be added as an extra cost option.

5.7. Environment Access

5.7.1. No direct customer access is provided to the hosted environment. Access is only via the Digital Repository application.

5.8. Database

5.8.1. A single database instance is deployed as part of the standard configuration.

5.9. Masking / Encryption

5.9.1. No masking or encryption of any data is provided as part of this service. It is not expected that the site will contain confidential data such as card data and as such not in scope for PCI rules.

5.10. Virus Checking

5.10.1. An industry standard application is used to virus check the servers. To avoid the impact of the introduction of faults with a new release, versions will generally be updated a short period after each standard release, although in the event of a deemed serious security risk, this may need to be implemented at short notice.

5.11. System Monitoring

5.11.1. The following tools are currently utilised to monitor and provide alerts on the health of the hosting environment.

Tool	Monitors	Detail
Solarwinds Virtualization Manager	VM Health & Performance	
Solarwinds Network Performance Monitor	Network Performance	
Nagios	Server & Network	
Panopta	Site Availability	Checks a specific site URL is accessible and loads in a timely manner outside of the Service Provider's network.

6. Service Provider Backup Service

6.1. Filesystem level backups of the service are performed to a local disk-based backup appliance, for which the weekly full dump is also exported to tape and stored offsite at a secure location 50+ miles away.

6.2. The filesystem backup allows for the basic recovery of the service in a disaster situation, but it not designed to permit the recovery of files due to user error or provide a more granular disaster recovery solution.

6.3. The service is included in all Digital Repository provided services and utilises a 3-week cycle / retention period. The cycle provides for a weekly full dump of the filesystem, with a daily incremental backup to capture changes since the last full dump. The weekly full dumps are retained for 3 weeks, the daily incremental backups for 2 weeks.

7. Website Penetration Testing

7.1. On initial setup of the service, installation may include the execution and correction of a Penetration (PEN) Test for the Service Offering. An external tool is used to identify and report on any vulnerabilities in the application or underlying service, or where poor code has been utilised. Any high risk / high impact issues will need resolution prior to the site being permitted to go live.

7.2. Further provision of PEN Testing is not included in the base service but can be requested as an optional additional chargeable service.

8. Service Provider Acceptable Use Policy

8.1. All Service Provider Managed Hosting Services are provided on the basis that the Customer conforms to the Acceptable Use Policy as detailed in this Service Level Agreement. All Services to a specific Customer will be suspended if that Customer breaches the Service Provider's Acceptable Use Policy.

8.2. The services provided by may not be used for any of the following activities.

8.2.1. The creation or transmission (other than for properly supervised and lawful research purposes) of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.

8.2.2. The creation or transmission of material which is designed or likely to cause annoyance, inconvenience, or needless anxiety.

8.2.3. The creation or transmission of defamatory material.

8.2.4. The transmission of material such that this infringes the copyright or other intellectual property rights of another person.

8.2.5. The transmission of unsolicited commercial or advertising material to other organisations.

8.2.6. Deliberate unauthorised access to facilities or services accessible via the Service Provider's network.

8.2.7. Intentional use of the provided services with any of the following characteristics:

8.2.8. corrupting or destroying other clients' data;

8.2.9. Disrupting the work of other clients; using the service in a way that denies service to other users, e.g. deliberate or reckless overloading of access links or of switching equipment;

8.2.10. Continuing to use a service after the Service Provider has requested that use cease because it is causing disruption to other clients

8.2.11. Other misuse of the Service Provider's services, such as the introduction of "viruses".

8.2.12. The creation or transmission of material which breaches the Data Protection Act or is otherwise unlawful.

8.3. Where access to the JANET network is achieved, any abuse of the acceptable use policy of that network (currently available at: https://community.jisc.ac.uk/library/acceptable-use-policy) will be regarded as unacceptable use of the Service Provider's service.

8.4. Where access to any other third party network is achieved, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of the service.

SCHEDULE 7

DIGITAL REPOSITORY – OFFSITE REPLICATION SERVICE

1. Service Overview

1.1. The Offsite Replication Service is not included as part of the base Digital Repository Service. This facility is only available when purchased as an additional extra cost option to the base service.

1.2. The Offsite Replication Service provides customers with assurance with regards to the long-term availability of the Service in the event of a disaster that severely affects the Service Provider's ongoing ability to run services out of its primary data centre in London.

2. Applicability

2.1. The resilience provided by this service applies purely to the Primary Live service only. It shall not include associated Services or environments. For example, Pre-Production, UAT, Reporting, Development, and Archive environments services, etc. are excluded from this replication.

3. Disaster Definition / Invocation

3.1. For the purpose of this Agreement, a Disaster is defined as an event that prevents the Service Provider from being able to deliver services from its primary data centre for a prolonged period of time, e.g. flood, fire, etc. For the avoidance of doubt, an event that results in a failure to meet availability commitments or incident resolution targets is not sufficient grounds to be termed a Disaster on its own.

3.2. Although invocation of running live from the Replicated Service will involve significant communication with the Customer, the final decision on whether an event is to be treated as a Disaster will be made by the Service Provider. This will be based on the Service Provider's assessment of the incident, including: severity, service impact, mitigation strategy, likely outage duration and risks to staff. Should the Data Centre remain in an operational condition, every effort will be made to continue running services from the facility using alternative arrangements on site.

3.3. Similarly, the timing of the invocation of this recovery process shall be decided by the Service Provider but with Customer agreement where possible.

4. Recovery Time Objective (RTO)

4.1. From the moment a Disaster is declared and the recovery process invoked, the target for services being fully restored to their pre-Disaster state shall be four (4) Business Hours.

5. Recovery Point Objective (RPO)

5.1. When the service is restored, the data on the restored service shall be no older than (24) hours prior to a Disaster being declared.

6. Service Failback

6.1. Service Failback from the Recovery site to the main production facilities will be carried out in a controlled manner and in consultation with the Customer. It is not possible to assign a specific timeframe KPI to failback, as this will be dependent on the duration and nature of the disaster event. The failback process and work flow will be arranged in advance and at an agreed maintenance window.

7. Service Data Centres

7.1. The target recovery Data Centre will be located at least 20km (straight line) from the primary data centre.

8. Service Contacts

8.1. All Offsite Replication Service queries and requests will be handled via the Service Provider's Service Desk and supported in line with their documented service levels agreements.

8.2. General queries and requests relating to the DR Service should be logged using the service desk and will be handled according to standard service prioritisation levels. Should a Customer have an urgent enquiry regarding a potential DR related incident they should log a "P1" (Priority 1) ticket with the relevant service desk, which will be escalated to the appropriate level.

8.3. The Customer must supply a list of nominated, responsible contacts (Name/email/phone number) that are stated in the service "Protection Template" documentation. A copy of this information will be kept by the Service Desk and securely off-site by the Service Provider's Senior Management Team. It is the Customer's responsibility to inform the Service Provider of any changes to their list of approved contacts.

9. Service Desk

9.1. The service is supported by the Service Provider's service desk. During office hours, the normal support contact points are provided.

9.2. Customers, who have a paid subscription to the Service Provider's Out-Of-Hours (OOH) support service, can also log P1 service tickets outside of normal business hours, in line with their standard service agreement. Agreed, nominated Customer contacts can contact the OOH support desk on:

Telephone: 0844 874 1369

10. Maintenance Window

10.1. The Service Provider operates a weekly maintenance window. During this period the Replication Service and site maybe partially or wholly unavailable. The timings and conditions around this window are as per the main service contract.

11. Customer Access to Infrastructure

11.1. Customers will not be provided with any access, physical or technological, to the infrastructure on which their Offsite Replication Service is provided.

12. Initial Implementation of Service

12.1. At contract start up the Service Provider will provide a day's support to review and test the replication service at their offices. This is likely to include a review of service boundaries, service operation review, DR process and configuration review (normal operation, testing, DR), service protection information required, Customer contacts, testing resources and customer responsibilities.

12.2. The review and testing will be at the Service Provider's offices at Senate House, Malet Street, London, WC1E 7HU during standard business hours, in-line with contracted service commitments. The customer must provide 20 days' notice to arrange and agree the meeting date to ensure appropriate availability of resources.

12.3. Should Customers wish to test from their own premises they will be responsible for the supply of their own test equipment, local and 3rd party infrastructure configuration and all timely correspondence with the Service Provider's administrative staff. Customer's will not be given access to the Service Provider's VMware console if they wish to test remotely.

12.4. Before the service is fully operational, the Service Provider and the Customer must complete and agree a Protection Template to document Offsite Replication Service resource interoperability (DNS and firewall port access) and Customer contact information.

12.5. It is the Customer's responsibility to ensure their local firewall and DNS records are maintained to support the service. The Customer is responsible for informing the Service Provider of any changes to their local configurations which may impact the service.

12.6. When the Office Replication service is first installed there will be an initial Seeding Period where the RTO and RPO commitments do not apply. This period maybe up to fourteen (14) days. The Customer will be informed of the anticipated end of this period at the start of the seeding.

13. Testing of the Offsite Replication Service

13.1. As part of the contract the Service Provider will provide one day's support for initial testing as part of the review meeting and after the first year, one day's support for an annual test of this service according to the terms of this schedule.

13.2. The test is solely aimed at testing the failover processes, the verification of customer remote VM Replica's and confirmation of data consistency.

13.3. The test does not include the following as standard:

13.3.1. Full failover of production services to run from the DR site, as this is highly disruptive and may result in data loss;

13.3.2. Failback testing, as it is implicit in the service solution.

13.4. Customers may request full failover and failback testing as an additional service option, which is chargeable.

13.5. The Service Provider will provide the following testing resources during this testing onsite:

13.5.1. A room for testing;

13.5.2. A test laptop;

13.5.3. Test failover of customer virtual machine replicas at the DR site, using the VMware console;

13.5.4. Utility server support by Service Provider's staff to demonstrate mail delivery;

13.5.5. Pre-populated DR Service DNS hosting as agreed in the protection template;

13.5.6. Pre-populated DR Service firewall access as agreed in the protection template;

13.5.7. Service Provider's support staff on call to answer queries;

13.5.8. Access to the JANET, to simulate external access to the DR site;

13.5.9. Reinstatement of the customer replicas from testing mode to live production status;

13.5.10. Basic test process log.

14. Customer Responsibilities

14.1. The Customer is responsible for the following:

14.1.1. Replication Service test scheduling and notification to the Service Provider;

14.1.2. Their own service test planning, auditing and documentation;

14.1.3. Pre-population and maintenance of local college firewall access rules for agreed ports;

14.1.4. Pre-population and maintenance of DNS CNAMES for service addresses;

14.1.5. Identification, documentation (and notification to the Service Provider) of all external service access dependencies and ports, e.g. LDAP services, Turnitin, plugins, etc;

14.1.6. Full disaster recovery support and integration of dependant services, not hosted or managed by the Service Provider.

14.1.7. Nomination of maintenance of customer contacts (2 x management and 2 x technical), who can be contacted throughout contracted support periods.

15. Service Provider Business Continuity

15.1. Service Provider disaster recovery, staff resources will be deployed in line with their Business Continuity policy. Depending on the nature of the event, support will be provided either from their main Offices, their Business Continuity Premises or remotely from staff home locations.

15.2. The service will be operated in line with the Service Provider's documented DR workflow and processes, which are available as part of the service documentation.

15.3. The Service Provider will assess options for replacing the facilities, should the Data Centre not be available for a prolonged period. The Service Provider will not, however commit to the provisioning of alternative production Data Centre resources, as part of the Offsite Replication Service.

15.4. Force Majeure shall apply, should the Service Provider be unable to staff the service as a result of a catastrophic event, which is beyond reasonable control.

16. Termination of Service

16.1. Subject to the notice period outlined in the Service Provider's standard Terms and Conditions and any other legal agreement between the parties, the Customer may notify the Service Provider of the intention to terminate the use of the Off-site Replication Service. The Customer shall provide to the Service Provider the final date on which they will use the service. The next Business Day after this will be termed the Termination Date. The Service Provider will acknowledge this notification within two (2) Business Days.

16.2. Customer access to the Office Replication Service will be removed at any time on or after the Termination Date. No response shall be provided to support cases on or after the Termination Date.

SCHEDULE 8

DIGITAL REPOSITORY – ARCHIVAL STORAGE SERVICE