LET'S GET DIGITAL

SERVICE LEVEL AGREEMENT (SLA)

1. PURPOSE

1.1 This SLA sets out the support the Service User will receive in the installation and maintenance of the Services, the resolution of any Faults and the responsibilities of the Service User to enable the efficient and reliable delivery of the Services. The SLA also identifies the target levels of Service Availability for each of the Services and the calculation of any Service Credits where this is not achieved.

1.2 This SLA does not apply to non-standard solutions or customised services unless this has been expressly agreed with the Service Provider.

1.3 Defined terms used in this SLA shall have the meaning given in the Agreement or as otherwise defined in the Appendix to this SLA.

2. OVERVIEW

2.1 The Service Provider delivers resilient and high availability services to thousands of customers across the UK. The Service Provider designs solutions that ensure its customers are not disrupted by outages. However, when a Fault occurs, the Service Provider will use reasonable endeavours to resolve it within the Service Availability targets set out in this SLA.

2.2 To minimise the risk of Unplanned Outages the Service Provider has ensured there is power protection in its datacentres and network aggregation points, and diverse routing within its carrier network. The Service Provider also offers a number of resilience options to ensure that disruption from Unplanned Outages are further reduced.

2.3 The Service Provider sources and provides market leading equipment that delivers high levels of reliability with industry leading "Mean Time Between Failure". However, the reliable operation of the Services is also dependent on the Service User complying with its responsibilities and adherence to the Acceptable Use Policy.

2.4 The strategies set out above enable the Service Provider to minimise costs and reduce the disruption to End Users of an Unplanned Outage.

3. CIRCUIT INSTALLATION

3.1 The Circuit supplied by the Service Provider provides the means of accessing the Services, including the internet via an IPVPN.

3.2 The Service Provider sources Circuits from telecommunications companies who plan the route for the fibre and conduct the necessary installation work to enable the delivery of the Services.

3.3 The target time for the installation of circuits is set out in the following table:

Circuit Type	Target Time
Fibre to the Service User	65 Working Days, subject to exceptions below
Fibre to the Cabinet and copper line to Service User	45 Working Days from point of order

3.4 The installation date will be confirmed following the conduct of a Site survey by the Supplier, which will provide an indication of when the Circuit will be ready for use by the Service User.

3.5 When ordering Circuits Service Users should note the possibility of unexpected delays and costs for the provision of the Service, which may require contingencies and alternative plans.

3.6 The provisioning of Circuits is a complex task that can be impacted by a number of factors that are outside of the Service Provider's reasonable control, including:

3.6.1 the availability of telecommunications network capacity in the area to install the Circuit. For example, there may be no space within a local distribution point such as a hubsite or a street cabinet;

3.6.2 blockages in ducts and trenches that carry the connections between different points on the network that require specialist skills to remove;

3.6.3 unexpected construction requirements, such as having to lay new cables underground or extend a duct to a property or specific location;

3.6.4 substandard equipment and assets, including telecommunications distribution points such as posts and street cabinets, which may need to be replaced or refreshed;

3.6.5 the requirement for appropriate permits and licences, such as wayleaves or highways access, that need to be granted by appropriate regulatory bodies; and

3.6.6 unexpected requirements for specialist technical information.

3.7 The installation of Circuits may be expedited in some circumstances but there is an additional cost for this service. Furthermore, a request to expedite does not guarantee delivery of a required target date because of factors which are not within the reasonable control of the Service Provider or its Supplier.

4. HOURS OF OPERATION

4.1 The Service Provider provides a range of options to ensure continued Service Availability, including:

4.1.1 network and security monitoring on a 24x7x365 basis;

4.1.2 the Help Desk operates between 08:00 – 18:00 on Working Days. Extended support hours are available subject to additional Charges; and

4.1.3 an emergency out of hours escalation service available for Multi Academy Trusts via a named service manager.

4.2 With the exception of Emergency Maintenance, Planned Maintenance will be conducted between 22:00 – 06:00. Notifications for Planned Maintenance will be provided at least 10 days before they occur.

4.3 Bespoke options for extending hours of operation are available to the Service User subject to additional Charges.

5. SUPERCHARGE SERVICES

5.1 Details of this Service are set out in the Service Descriptions.

5.2 The Service is designed to minimise the risk of Unplanned Outages and provide a level of reliability to End Users in line with our targets and expectations. However, there can be circumstances where Service Availability is affected by developments outside the control of the Service Provider or its Suppliers, including:

5.2.1 major and prolonged power outages of utility providers;

5.2.2 accidental damage to cabling and supporting infrastructure due to civil engineering works;

5.2.3 Unplanned Outages in networks linked to the Services, including other telecommunications providers;

5.2.4 rodent infestations in trenching and ducting;

5.2.5 flooding; and

5.2.6 the malicious actions of third parties, including cybersecurity attacks.

5.3 The Services provide mitigation against Unplanned Outages through:

5.3.1 power protection at aggregation points within the network such as datacentres and regional distribution points;

5.3.2 resilient and diverse routing in the carrier network;

5.3.3 high availability design for critical equipment, including redundant components;

5.3.4 multiple ingress and egress points to the internet;

5.3.5 24 x 7 network monitoring supported by an emergency out of hours service;

5.3.6 24 x 7 security monitoring; and

5.3.7 technical countermeasures to reduce the risk of successful security attacks on the Services.

5.4 These steps enable the Service Provider to deliver high levels of service to the Service User's IPVPN Circuits. For Circuits that are not provided via the Service Provider's IPVPN, the Service Provider will make reasonable efforts to resolve outages to the same targets.

5.5 The target Service Availability for SuperCharge Services are set out below:

Site Connection Type	Target Availability
Single Circuit	99.95%
Single Circuit with xDSL or ISDN backup on same CE device	99.95%
Single Circuit with xDSL or ISDN backup on different CE devices	99.95%
Dual Circuits, dual CEs to separate PE Routers (PoPs)	99.99%
Dual Circuits, dual CEs to separate PE Routers with planned diversity of the access circuit	99.995%

5.6 With respect to packet loss and latency, the maximum target packet loss and latencies are set out below:

	Packet Loss (%)	Latency (ms)
Service Level	0.2	250

6. SUPERCLOUD SERVICES

6.1 Details of this Service are set out in the Service Descriptions.

6.2 The Service Provider provides secure private cloud services that are hosted in UK datacentres that conform to the requirements of the Data Protection Legislation.

6.3 The Service Provider serves thousands of customers and its datacentre resources and services are generally, though not exclusively, replicated across multiple Sites, providing high availability and continuous operation wherever possible.

6.4 The target availability of SuperCloud Services is set out in the table below:

Service	Target Availability
LGfL Email	99.95%
LGfL Backup	99.95%

7. CYBERCLOUD SERVICES

7.1 Details of this Service are set out in the Service Descriptions.

7.2 The Service Provider operates a highly secure network that is designed to minimise threats and risks to customers. This includes a defence in depth strategy that reduces and mitigates risk within the network and provides protection against malicious activity.

7.3 By protecting Service Users with multiple levels of defence, the Service Provider makes it more difficult for security threats to occur.

7.4 The target availability for CyberCloud services are set out in the table below:

Service	Target Availability
LGfL Mail Scanning Service	99.95%
LGfL Core Network Firewall Availability	99.95%
Edge Firewall Availability	99.5%
Distributed Denial of Service (DDoS) Remediation	90% within 1 hour 95% within 1 working day

7.5 The Service Provider provides a firewall for the Service User and a firewall in the network core. The Service Provider's firewall has a rule set that is designed to minimise risk. Service Users can change the rules on the Service Provider's firewall or choose not to use it.

7.6 The network is continuously monitored for security threats and the Service Provider receives alerts when exceptions occur, such as the identification of a malicious virus signature.

7.7 Periodically, the Service Provider will alert customers of potential malicious activity on the network, including viruses, malicious code and potentially fraudulent activity. The Service Provider may require the Service User to undertake follow-up activity to resolve issues and notifications sent as provided in the Acceptable Use Policy.

8. DIGISAFE SERVICES

8.1 Details of this Service are set out in Service Descriptions.

8.2 The Service Provider provides filtering and a range of network services to keep children safe. The filtering solution is designed for high availability and the protection of children. In the event that the filtering services fail, access to the internet will be blocked across the network to prevent unauthorised access to inappropriate content.

8.3 The filtering service connects to other agencies to ensure that the filtering services are operating with the most up to date block and deny lists. The Service Provider may share information with law enforcement agencies where it is required to do so.

Service	Target Availability
LGfL Filtering Service	99.95%

9. TECHSQUAD SERVICES

9.1 The TechSquad provides a range of support to End Users to support the resolution of Faults and to resolve Service requests, including providing advice and supporting changes.

9.2 The Help Desk includes:

9.2.1 a telephone support line;

9.2.2 on-line support available 24 hours a day, 365 days a year to log incidents, change requests and requests for advice;

9.2.3 a case management system to enable tracking of Faults and Service requests; and

9.2.4 a support site that provides updates and notifications of key events or any outages impacting customers.

9.3 The Service Provider will provide reasonable endeavours to:

9.3.1 answer 90% of telephone calls to the Help Desk within 5 rings;

9.3.2 resolve 70 % of telephone call to the Help Desk at the first point of contact; and

9.3.3 respond to complaints regarding Service Provision within 5 Working Days.

10. FAULT REPORTING

10.1 The Service User shall, as soon as possible after the Commencement Date notify the Service Provider of the members of its staff with authority to report Faults. Any replacement to its nominated contacts must be notified to the Service Provider as soon

as possible. The Service User warrants that such individuals shall have sufficient knowledge to understand the nature of any Faults and will be able to assist the Service Provider and its agents to assess and resolve them.

10.2 Faults must be reported to the Help Desk by the Service User's nominated contact. This ensures that a Fault can be managed and resolved efficiently. The Service Provider will not acknowledge or attend to any Fault reports made by a person other than the nominated contact unless there are exceptional circumstances.

10.3 The information needed by the Service Provider to resolve a Fault includes:

10.3.1 Site name;

10.3.2 Site number / DfE code;

10.3.3 details of Fault Site;

10.3.4 name of nominated contact;

10.3.5 time the Fault commenced;

10.3.6 nature and details of Fault; and

10.3.7 further contact details if required.

10.4 The Service User must provide the Fault reference number in any further communications following its initial report.

10.5 In order for Unplanned Outages to be resolved efficiently, Service Users may be required to undertake triage that will enable the Service Provider and its Suppliers to pinpoint the source of the problem and ensure that appropriate engineering resources are dispatched to Site. This triage may involve:

10.5.1 confirming that there are no power issues at the Site or the local area which may be disrupting equipment;

10.5.2 confirming that the equipment is switched on; and

10.5.3 providing information displayed on any relevant equipment, including the condition of any status lights.

10.6 Faults may take longer to resolve if triage is not undertaken when requested.

10.7 Unless authorised by the Service Provider, the Service User must not contact the Service Provider's or Supplier's engineers, technicians or other agents regarding a Fault. The Service Provider may authorise a competent representative of the Service User to have direct contact with the Supplier's staff in order to facilitate the resolution of a specific fault. The Service Provider may charge the Service User for unauthorised contact.

11. FAULT PRIORITIES

11.1 Faults reported to the Help Desk are categorised into priorities with different response times depending on the seriousness and impact of the Fault.

11.2 The following table contains examples of the different Fault priorities:

Priority 1	A major service is down or unavailable resulting in total or major loss of IT capabilities at a Site, including: • loss of the Service; • severe latency / degradation which is rendering the Services unusable; • health and safety risk; or • a material risk that a serious safeguarding harm may arise. A major incident will be triggered in the event of an incident causing loss of service across multiple sites.
Priority 2	A major service is suffering from severe performance issues but is still functioning at a Site. The impact on a Site is significant though may be affecting only a limited number of Sites, including: • partial loss of the Services or an intermittent connection; or • severe latency where the Service remains usable.
Priority 3	A service is suffering from poor performance and is affecting a limited number of Sites, including: • performance relating to latency; • slow connection speeds or equivalent performance issues; or • inaccessible resource which is not vital to daily activities.
Priority 4	A Site requires assistance, advice or guidance in relation to the use of a Service, including: • request for information about a Service; • advice on how to configure a Service; and • advice on how to make best use of a Service.

12. FAULT RESPONSE, SERVICE REQUESTS AND SERVICE RESTORATION

12.1 The Service User may request advice regarding a Service, how to configure a Service and where to find further information at any time between 08:00 – 18:00 of any Working Day.

12.2 The Service User accepts that the time to respond to and restore the Services commences from the report of the Fault by the Service User and ends when details of the resolution have been provided to the Service User. The Service User acknowledges and accepts that the response and resolution times may be suspended if it requires an engineer to attend on Site to resolve the Fault.

12.3 The Service Provider operates using an internal escalation procedure so that appropriate resources can be applied if problems are not resolved within the relevant resolution time.

12.4 The Service User shall provide the Service Provider and its Suppliers with full and continuous access to its network equipment for diagnostic and fault rectification purposes and shall not unreasonably refuse to allow reasonable down time necessary to restore the Service.

12.5 The Service Provider will use reasonable endeavours to respond within 4 hours of the report of a fault and to rectify it in accordance with the following targets:

Priority Level	Target Response Time	Target Fix Time	Hours of Operation
Priority 1	90% in 4 hours	90 % in 6 Hours	08:00 – 18:00
Priority 2	90% within 4 hours	90 % in 8 Hours	08:00 – 18:00
Priority 3	90% within 4 hours	100% in 3 Working Days	08:00 – 18:00
Priority 4	90% in 4 hours	95% of firewall change requests within 1 working day 95 % of urgent URL blocking / unblocking within 1 working day 95% of password resets within 1 working day 95% of all other requests within 5 Working Days	08:00 – 18:00

12.6 The Service Provider may charge the Service User for any diagnosis, repair, restoration or remedial work carried out by the Service Provider as the result of an Excused Outage.

12.7 The Service Provider will seek to resolve regular intermittent outages of short duration, once identified, by means of a Service Improvement Plan to diagnose and resolve the root cause of the Fault.

13. FAULT ESCALATION

13.1 Subject to paragraph 13.2, if a Fault is not resolved within the target fix timescales, Service Users may escalate the issue in accordance with the following table:

Escalation Level	Escalated To		Time Elapsed
	Service Provider	Service User	
1	Service Desk Manager	School IT Network Managers	By target fix time for priority
2	Service Manager	Schools IT Manager	By target fix time for priority +2 hours
3	CEO	European IT Director	By target fix time for priority +16 hours

13.2 In exceptional circumstances where a delay in the Fault resolution process set out in paragraph 12 would or is likely to cause significant disruption to the Service User, the Service User may escalate the issue direct to the Service Provider's service manager.

14. SERVICE AVAILABILITY MEASUREMENT

14.1 Service Availability is measured as a percentage of the total time the Service is not available in a calendar month in accordance with the following formula:

$$Service\ Availability = \frac{TU - NO}{TU}\ x\ 100\%$$

Where:

TU = target uptime in calendar month for the relevant Service less any Planned Maintenance or Excused Outage

NO = the network outage time recorded by the network management system at the Help Desk

14.2 The Service User acknowledges and agrees that the Help Desk's record represents the network outage time for the purpose of calculating Service Availability. Reports on Service Availability will be produced on request by prior agreement but not more than once per month.

14.3 Where the Services include resilience, a Fault on a single Circuit will not be counted for the purposes of Service Availability if the Service is still available via the resilient Service.

15. SERVICE CREDITS

15.1 Provided the Service User has satisfied its responsibilities, the Service Provider will provide Service Credits if the Service Availability for any Circuit falls below the target availability for that Circuit as set out in the table in paragraph 5.5 (provided that any Circuit that is delivered over a copper-based connection shall have target availability of 99.95%).

15.2 Service Credits are calculated at the rate of 10% of the monthly rental for the affected Service in respect of each affected Service Order for each month which the Service does not meet the Service Availability target.

15.3 Service Credits are not be available to the extent that the Service Provider failed to meet the Service Levels due to:

15.3.1 the suspension or termination of the Services in accordance with the terms of the Agreement, including any non-compliance with the Acceptable Use Policy;

15.3.2 the non-availability of a Service as a result of an Excused Outage; or

15.3.3 a failure or delay by the Service User when complying with its responsibilities, including when responding to a request to triage a Fault or providing full and continuous access to its network equipment.

15.4 Service Credits are a credit against the Charges and do not include VAT. The Service Provider shall shall calculate any Service Credit that is due and shall automatically deduct any Service Credit from the next and, if applicable, subsequent invoices payable by LGfL. If no further Charges fall due after any Service Credits accrue, the Service Provider shall issue a credit against the previous invoice.

15.5 The Service User acknowledges and accepts that Service Credits are its sole and exclusive remedy with respect to the Service Provider's failure to meet the Service Levels.

15.6 Notwithstanding any provisions in the Agreement, including this SLA, to the contrary, in no event shall the total amount of any Service Credits provided in any calendar month exceed the Charges for the affected Service for the same month.

16. SERVICE USER RESPONSIBILITIES

16.1 The success of the Services relies on an effective partnership between the Service User and Service Provider that is mutually supportive and respectful.

16.2 A key requirement during the installation of a new Circuit is for the Service User to work with the Service Provider's nominated technical support contact to "on board" the Site successfully. If these onboarding processes are not followed, provisioning of the Services may be delayed, the Service User may be unable to take full advantage of the Services and products provided and the Services may be under-utilised.

16.3 Onboarding of the Services will require:

16.3.1 the supply of technical information to enable the provisioning of the Services;

16.3.2 the provision of contact information to enable efficient communication between the Service Provider, the Supplier and the Service User; and

16.3.3 subscription to key support resources to enable the Service User to receive information relating to service support and service developments.

16.4 Service Users will need to ensure that their Local Area Network has sufficient capacity to enable it to connect to the Services, including installation of network equipment.

16.5 Service Users are required to adhere to the Service User's obligations under the Agreement and the Acceptable Use Policy.

16.6 In order to benefit from the full range and functionality of the Services, the Service User will need to integrate the MIS systems for each school with Unified Sign On.

16.7 Service User will need to ensure that staff receive adequate training to enable the appropriate use of the services and access to the support service.

APPENDIX A - DEFINITIONS

"Circuit"	means the physical network connection over which the Services are provided;
"Emergency Maintenance"	means any unplanned maintenance conducted by the Supplier in respect of an incident that has occurred or to prevent an incident from occurring;
"End Users"	means the Service User's schools and other end users of the Services, including the Service User where the context requires;
"Excused Outage"	means any downtime directly caused by: (a) elements of the Service User's network or system, or any part of it not supplied by or on behalf of the Service Provider; (b) a fault in, or any problem associated with equipment connected on the Service User's side of the network; (c) acts or omissions by or on behalf of the Service User; (d) breach of the Agreement by the Service User; (e) failure or delay to comply with the reasonable instructions of the Service Provider or its agents; (f) refusal to allow Service Provider employees, agents or sub-contractors to enter the Service User's premises to diagnose or remedy any Fault; (g) Emergency Maintenance (unless conducted between 08:00 – 18:00 of any Working Day); (h) an event of force majeure; or (i) any other act or omission of a third party which is beyond the reasonable control of the Service Provider, including cutting a network cable;
"Fault"	means a Service outage/downtime or a fault relating to the Service;
"Help Desk"	means the support call centre operated by or on behalf of the Service Provider to which Faults and any other service requests are submitted;
"IPVPN"	means a virtual private network provide over the internet;
"Network Outage Time"	means the total of the outage duration during which a Site is unable to transmit or receive data to or from other Sites via the Service in a calendar month. Such measurements are made based on the equipment and associated tail circuit relating to the Service;

“Planned Maintenance”	means any downtime: (a) scheduled by the Service Provider or the Supplier to carry out any preventative maintenance or upgrades to the Service or communications network; or (b) caused by any Services requested or approved by the Service User, including network redesign or reconfiguration;
“Service Availability”	has the meaning give in paragraph 14.1 of this document;
“Service Level”	means the service levels set out in this document; and
“Unplanned Outages”	means the Service is not available for use by the Service User.