



## UNITED NET CONNECT SERVICE LEVEL AGREEMENT, TECHNICAL SUPPORT, ESCALATION & REMEDIAL PROCEDURES

### PREFACE

The **UNITED NET CONNECT** managed service, for primary and Junior schools, is a wholly owned division of leading cyber security Distributor and software vendor, United Network Technologies Limited.

United Network Technologies has offices in Chelmsford, Essex and Princes Risborough, Buckinghamshire. It has established itself as a leading value-added distributor (VAD) and managed service provider (MSP) that works on a one-to-one basis with their select Premier Reseller partners and with their clients.

The company supply Cloud, Network, Web including Browser Isolation tools, Email and Mobile Cyber Security technologies via its Channel and is recognised for its ability to seamlessly integrate products creating holistic solutions across a variety of industry sectors covering Professional Services, Banking & Finance, Education, Public Sector and some SMB markets.

The company also offers a specialist managed service to all UK Primary and Secondary schools comprising inexpensive internet connections (connectivity pricing specially negotiated on behalf of all UK schools with mainstream industry carriers), PLUS, we have added our award-winning cyber security suite, known as **School-Secure**, containing industry strength, age-appropriate Web (Content) Filtering, Endpoint with Classroom Management, Email Filtering, 2Factor authentication, optionally with Anti-virus and/or automatic Online Backup.

Our premier resellers are innovative, forward thinking, creative and expertly trained each to our vendors specific accredited standards and beyond. Flanking our growing array of valued partners is a proven and committed internal sales and technical team who are on-hand to assist the cultivation of both new and renewable business opportunities, and deal with installation and technical support issues.

This enclosed document entitled the 'Service Level Agreement' herein, referred to as the "Schedule", is a technical support and service level agreement (SLA) which details the service levels a customer should expect from our award-winning **School-Secure** managed service. Should our service become faulty in any way throughout the duration of our agreement, our service allows each school a number of associated service credits throughout each 'service-year' which can be redeemed upon reaching an anniversary date (or renewal date) and applied to a schools forthcoming term (year) or renewable agreement for the **School-Secure** Managed Service which can be transferred and become an additional discount for primary schools. This document also details Performance Monitoring with Service Reporting.

**\*\*** - Please note, this agreement has been compiled for the benefit, and in favour of, our school customers and not the Vendor, i.e. United Net Connect, the Supplier?



United Network Technologies is a specialist distributor for an extensive range of Cloud-only cyber security services and solutions into Commerce, Education and Public-sector markets which include many NHS Trusts, London Borough Councils, Legal Firms, Lloyds Insurance institutions and over 3,500 schools, colleges and universities.

\*\*\*\*\*

## 1. DEFINITIONS AND INTERPRETATION

- 1.1 In this Contract of Terms & Conditions for the ***School-Secure*** managed service, unless the context otherwise requires, denoted expressions shall have the meanings set out in Schedule 1 (Definitions).
- 1.2 If an expression does not have an interpretation in Schedule 1 (Definitions) or relevant Schedule, it shall have the meaning given to it in the Framework Agreement. Otherwise, it shall be interpreted in accordance with the dictionary meaning.
- 1.3 In this Contract, unless the context otherwise requires:
  - 1.3.1 the singular includes the plural and vice versa;
  - 1.3.2 reference to a gender includes the other gender;
  - 1.3.3 references to a person include an individual, company, body corporate, corporation, unincorporated association, firm, school, trust, educational institution, partnership or other legal entity;
  - 1.3.4 references to “writing” include typing, printing, lithography, photography, display on a screen, electronic and facsimile transmission and other modes of representing or reproducing words in a visible form, and expressions referred to in writing shall be construed accordingly;
  - 1.3.5 references to “representations” shall be construed as references to present facts, to “warranties” as references to present and future facts and to “undertakings” as references to obligations under this Contract;
  - 1.3.6 references to “Clauses” and “Schedules” are, unless otherwise provided, references to the clauses and schedules of this Contract and references in any Schedule to parts, paragraphs, annexes and tables are, unless otherwise provided, references to the parts, paragraphs, annexes and tables of the Schedule in which these references appear;
- 1.4 Any permitted changes by the Customer to the template terms and the template Form under Clause 4 (Procedure) of the Framework Agreement and Framework Schedule 5 (Procedure) prior to them becoming the terms and the form and the Parties entering this Contract shall prevail over the Framework Agreement.
- 1.5 Where the Framework Schedule (Tender) contains provisions which are more favourable to the Customer in relation to this Contract, such provisions of the Tender shall prevail. The Customer shall in its absolute and sole discretion determine whether any provision in the Tender is more favourable to it in this context.



### SCHEDULE 1: DEFINITIONS

In accordance with this document and its profiles (Definitions and Interpretations) of this Contract including its recitals the following expressions shall have the following meanings:

<b>"Advanced Persistent Threat Attacks"</b>	means a set of stealthy and continuous computer hacking processes, often orchestrated by human(s) targeting a specific entity. An advanced persistent threat (APT) usually targets organisations and/or nations for business or political motives. APT processes require a high degree of covertness over a long period of time. The "advanced" process signifies sophisticated techniques using malware to exploit vulnerabilities in systems. The "persistent" process suggests that an external command and control system is continuously monitoring and extracting data from a specific target. The "threat" process indicates human involvement in orchestrating the attack;
<b>"Affiliates"</b>	means in relation to a corporate body or school, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control of that body from time to time such as a Trust or Academy Trust;
<b>"United Net Connect Services"</b>	means the Service Component that enables the on-boarding and connection of Consumer Network Service to the <b>School-Secure</b> main managed service;
<b>"United Net Connect Implementation Services"</b>	means the United Net Connect Service Component that is configured by a Reseller Partner or by United Network Technologies;
<b>"United Net Connect Disconnection Services"</b>	means the Service Component that enables the disconnection of United Net Connect Managed Service;
<b>"Approval"</b>	means the prior written consent of the Customer and <b>"Approve"</b> and <b>"Approved"</b> shall be construed accordingly;
<b>"Available"</b>	means the extent to which the United Net Connect Managed Service is available. A Service Component shall be available when it is performing, or capable of performing, all of the functions it is intended perform and shall be construed accordingly;
<b>"Average Latency"</b>	means is the delay incurred as a result of the processing by the United Net Connect Managed Service. Measurement shall be between the inbound and outbound internet boundaries of the



United Network Technologies is a specialist distributor for an extensive range of Cloud-only cyber security services and solutions into Commerce, Education and Public-sector markets which include many NHS Trusts, London Borough Councils, Legal Firms, Lloyds Insurance institutions and over 3,500 schools, colleges and universities.

	United Net Connect Managed Service supplied to the customer;
<b>"Blacklist"</b>	Blacklists provide information regarding Internet locations that are deemed as "bad", used to disallow access to the locations identified;
<b>"Blocking rules"</b>	means the configuration deployed on the United Net Connect Managed Service that restricts pertaining traffic from reaching the Internet or the response reaching the originator preventing, for example, communication with a Command and Control server;
<b>"Botnet Traffic"</b>	a) means artificial traffic generated from infected zombies PCs and aiming, among other things, at generating fraudulent advertising revenue through click fraud and impression fraud;
<b>"Services Contract"</b>	means a legally binding agreement (entered into pursuant to the provisions of the Framework Agreement) for the provision of the Services made between a Contracting Body (the school, Trust, PSN) and the Supplier;
<b>"Services Commencement Date"</b>	means the date of commencement of this Contract;
<b>"United Net Connect Managed Service Contract Charges"</b>	means the prices (inclusive of any Milestone Payments and exclusive of any applicable VAT), payable to the Supplier by the school, Trust, Representing Body, PSN under this Contract;
<b>"Service Contract Period"</b>	means the term of this Contract from the Commencement Date until, and including, the Expiry Date;
<b>"Contract Year"</b>	means a consecutive period of twelve (12) Months commencing on the Commencement Date or each anniversary thereafter;
<b>"Expiry Date"</b>	means: a) the end date of the Initial Period or any Extension Period; or if this Contract is terminated before the date specified in (a) above, the earlier date of termination of this Contract applies;
<b>"Extension Period"</b>	means the extension term of this Contract from the end date of the Initial Period to the end date of the extension period;

<b>"Change in Law"</b>	means any change in Law which impacts on the supply of the Services and performance of the Terms which comes into force after the Commencement Date;
<b>"Commercially Sensitive Information"</b>	means the Confidential information listed in the Order Form (if any) comprising of commercially sensitive information relating to the Supplier, its IPR or its business or which the Supplier has indicated to the Customer that, if disclosed by the Customer, would cause the Supplier significant commercial disadvantage or material financial loss;
<b>"Confidential Information"</b>	means the Customer's Confidential Information and/or the Supplier's Confidential Information, as the context specifies;
<b>"Continuous Improvement Plan"</b>	means a plan for improving the provision of the United Net Connect Services and/or reducing the Charges produced by the Supplier;
<b>"Customer"</b>	means the primary school(s) identified in the Order Form;
<b>"Customer Data"</b>	means: <ul style="list-style-type: none"><li>a) the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, including any Customer's Confidential Information, and which:<ul style="list-style-type: none"><li>i) are supplied to the Supplier by or on behalf of the Customer; or</li><li>ii) the Supplier is required to generate, process, store or transmit pursuant to this Contract; or</li></ul></li></ul> any Personal Data for which the Customer is the Data Controller or the Data Processor;
<b>"Customer Premises"</b>	<ul style="list-style-type: none"><li>a) means premises owned, controlled or occupied by the Customer which are made available for use by the Supplier or its Sub-Contractors for provision of the Services (or any of them);</li></ul>
<b>"Customer Property"</b>	means the property, other than real property and IPR, including the Customer System issued or made available to the Supplier by the Customer in connection with this Contract;
<b>"Customer Representative"</b>	means the representative appointed by the Customer from time to time in relation to this Contract;

<b>"Customer Software"</b>	means any software identified as such in the Order Form together with all other software which is not identified as such in the Order Form but which is owned by or licensed to the Customer and which is or will be used by the Supplier for the purposes of providing the Services;
<b>"Customer System"</b>	means the Customer's computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the Customer or the Supplier in connection with this Contract which is owned by or licensed to the Customer by a third party and which interfaces with the Supplier System or which is necessary for the Customer to receive the Services;
<b>"Data Controller"</b>	has the meaning given to it in the General Data Protection Legislation;
<b>"Data Processor"</b>	has the meaning given to it in the General Data Protection Legislation;
<b>"Data Protection Legislation"</b>	a) means applicable legislation protecting the fundamental rights and freedoms of individuals, in respect of their right to privacy and the processing of their personal data, as amended from time to time, including the General Data Protection Regulation and the Privacy and Electronic Communications Regulations 2003, together with decisions, guidelines, guidance notes and codes of practice issued from time to time by courts, data protection authorities and other applicable Government authorities;
<b>"Data Subject"</b>	has the meaning given to it in the General Data Protection Legislation;
<b>"Data Subject Access Request"</b>	means a request made by a Data Subject in accordance with rights granted pursuant to the General Data Protection Legislation to access his or her Personal Data;
<b>"Deductions"</b>	means all Service Credits, Delay Payments or any other deduction which the Customer is paid or is payable under this Contract;
<b>"Default"</b>	means any breach of the obligations of the Supplier (including but not limited to including abandonment of this Contract in breach of its terms) or any other default (including material Default) after the words, act, omission, negligence or

	statement of the Supplier, of its Sub-Contractors or any Supplier Personnel howsoever arising in connection with or in relation to the subject-matter of this Contract and in respect of which the Supplier is liable to the Customer;
<b>"Defect"</b>	<p>means any of the following:</p> <ul style="list-style-type: none"><li>a) any error, damage or defect in the manufacturing of a Deliverable; or</li><li>b) any error or failure of code within the Software which causes a Deliverable to malfunction or to produce unintelligible or incorrect results; or</li><li>c) any failure of any Deliverable to provide the performance, features and functionality specified in the requirements of the Customer or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from passing any Test required under this Contract; or</li></ul> <p>any failure of any Deliverable to operate in conjunction with or interface with any other Deliverable in order to provide the performance, features and functionality specified in the requirements of the Customer or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from passing any Test required under this Contract;</p>
<b>"Delay"</b>	<p>means:</p> <ul style="list-style-type: none"><li>a) a delay in the Achievement of a Milestone by its Milestone Date; or</li></ul> <p>a delay in the design, development, testing or implementation of a Deliverable by the relevant date set out in the Implementation Plan;</p>
<b>"Delay Period Limit"</b>	shall be the number of days specified in Part A of Schedule 4: Implementation Plan, Customer Responsibilities and Key Personnel, for the purposes of <b>Error! Reference source not found.</b> ;
<b>"Deliverable"</b>	means an item or feature in the supply of the Services delivered or to be delivered by the Supplier at or before a

	Milestone Date listed in the Implementation Plan (if any) or at any other stage during the performance of this Contract;
<b>"Delivery"</b>	means, in respect of the Services, the time at which the Services have been provided or performed by the Supplier as confirmed by the issue by the Customer of an Assurance Certificate in respect of the relevant Milestone thereof (if any) or otherwise in accordance with this Contract and accepted by the Customer and <b>"Deliver"</b> and <b>"Delivered"</b> shall be construed accordingly;
<b>"Denial of Service"</b>	means an interruption in authorised user's access to a computer network, typically one caused with malicious intent;
<b>"Disaster"</b>	means the occurrence of one or more events which, either separately or cumulatively, mean that the Services, or a material part thereof will be unavailable (or could reasonably be anticipated to be unavailable for the period specified in the Order Form as the Recovery Time Objective);
<b>"Disaster Recovery Services"</b>	means the services embodied in the processes and procedures for restoring the provision of Services following the occurrence of a Disaster, as detailed further in Schedule 10 (Business Continuity and Disaster Recovery);
<b>"Dispute"</b>	means any dispute, difference or question of interpretation arising out of or in connection with this Contract, including any dispute, difference or question of interpretation relating to the Services, failure to agree in accordance with the Variation Procedure or any matter where this Contract directs the Parties to resolve an issue by reference to the Dispute Resolution Procedure;
<b>"Framework Agreement"</b>	means the framework agreement between the Authority, School and the Supplier referred to in the Order Form;
<b>"Framework Commencement Date"</b>	means the date of commencement of the Framework Agreement as stated in the Schedule 1 (Definitions);
<b>"Framework Period"</b>	means the period from the Framework Commencement Date until the expiry or earlier termination of the Framework Agreement;
<b>"General Data Protection Regulation" or "GDPR"</b>	means Regulation 2016/8 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, together with the codes of practice, codes of conduct,



	regulatory guidance and standard clauses and other related legislation resulting from the GDPR, as updated from time to time;
"Help Desk"	means the single point of contact help desk set up and operated by the Supplier for the purposes of the <b>School-Secure</b> managed service from United Net Connect;
"Implementation Plan"	means the plan set out in paragraph 2.4 of the Order Form;
"Information"	has the meaning given to it under section 84 of the Freedom of Information Act 2000;
"Internet filtering (or Web or Content filtering)"	means the mechanism by which Content-control software is used to restrict or control the content a reader is authorised to access, for example; when utilised to restrict material delivered over the Internet via the Web, e-mail, or by other means. Content-control software determines what content will be available or perhaps more often what content will be blocked;
"Internet-bound traffic filtering"	a) means the application of rules configured on the United Net Connect Service to traffic originating from a web connection having a destination address located on the customers internet and the traffic returned in response;
"IP Records"	means the dataset of all IP addresses assigned to each of the Customers/entity/third party, this dataset contains the following fields: <ul style="list-style-type: none"><li>- SIN (Service Identification Number)</li><li>- IP Address</li><li>- Subnet Mask</li><li>- Organisation Name</li><li>- ODS Code;</li></ul>
"Key Performance Indicators" or "KPIs"	means the performance measurements and targets in respect of the Supplier's performance of the Agreement;
"Know-How"	means all ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the Services but excluding know-how already in the other Party's possession before the Commencement Date;

<b>"Licensed Software"</b>	means all and any Software licensed by or through the Supplier, its Sub-Contractors or Reseller Partners or any third party to the Customer for the purposes of or pursuant to this Contract, including any Supplier Software, Third Party Software and/or any Specially Written co-existence Software;
<b>"Log Information"</b>	means, complete and accurate threat event logging data including, but not be limited to, for each occurrence of the events identified including: <ul style="list-style-type: none"><li>- the source of the message;</li><li>- the destination of the message;</li><li>- the triggering ruleset and/or signature and/or pattern;</li><li>- date time stamps associated with receipt and response;</li></ul>
<b>"Malicious Software"</b>	means any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence;
<b>"Operating Environment"</b>	a) means the Customer or Schools System and the Sites;
<b>"Operational Change"</b>	any change in the Supplier's operational procedures which in all respects, when implemented: <ul style="list-style-type: none"><li>a) will not affect the Charges and will not result in any other costs to the Customer;</li><li>b) may change the way in which the Services are delivered but will not adversely affect the output of the Services or increase the risks in performing or receiving the Services;</li><li>c) will not adversely affect the interfaces or interoperability of the Services with any of the Customer's IT infrastructure; and</li></ul> will not require a change to this Contract.
<b>"Operational Hours"</b>	means 8 hours a day, 5 days a week less Bank Holiday;
<b>"Order"</b>	means the order for the provision of the United Net Connect Services placed by the Customer with the Supplier in accordance with the terms of this Contract;

<b>"Order Form"</b>	means the form, as completed and forming part of this Contract, which contains details of an Order, together with other information in relation to such Order, including without limitation the description of the Services to be supplied;
<b>"Personal Data"</b>	has the meaning given to it in the General Data Protection Legislation;
<b>"Personal Data Breach"</b>	has the meaning given to it in the General Data Protection Legislation;
<b>"Quarter"</b>	means three-months. The first three Service Periods and each subsequent three Service Periods (save that the final Quarter shall end on the date of termination or expiry of an anniversary date or entire Contract);
<b>"Sandboxing"</b>	a) means testing the item in an isolated environment in order to determine if there is malicious intent;
<b>"Service Failure"</b>	b) means an unplanned failure and interruption to the provision of the Services, reduction in the quality of the provision of the Services or event which could affect the provision of the Services in the future;
<b>"Severity 1 Service Incident"</b>	a Service Incident which, in the reasonable opinion of the Customer; (a) constitutes a loss of the Service which prevents any web traffic from routing correctly;  (b) has a critical impact on the activities of a Service Use; or  (c) causes significant financial loss and/or disruption to a Service User.  Or, rulesets for all cannot be updated
<b>"Severity 2 Service Incident"</b>	a Service Incident which, in the reasonable opinion of the Customer has the potential to: (a) have a major (but not critical) adverse impact on the activities of a Service User and no workaround acceptable to the Service User is available; or  (b) cause a financial loss and/or disruption to a Service User which is more than trivial but less severe than the significant

	<p>financial loss described in the definition of a Severity 1 Service Incident;</p> <p>Or, rulesets for one or more (but not all) cannot be updated</p>
"Severity 3 Service Incident"	<p>a Service Incident which, in the reasonable opinion of the Customer has the potential to:</p> <p>(a) have a major adverse impact on the activities of a Service User which can be reduced to a moderate adverse impact due to the availability of a workaround acceptable to the Service User; or</p> <p>(b) have a moderate adverse impact on the activities of a Service User;</p> <p>Non-exhaustive example: Internal reporting capability is not available or is inaccurate</p>
"Severity 4 Service Incident"	<p>a Service Incident which, in the reasonable opinion of the Customer has the potential to have a minor adverse impact on the provision of the Services to a Service User.</p> <p><b>Non-exhaustive example:</b> No Coaching pages or messages displayed to end users notifying them of a block which has taken place</p>
"Severity 5 Service Incident"	<p>a Service Incident which, in the reasonable opinion of the Customer has the potential to have a very minor adverse impact on the provision of the Services to a Service User;</p> <p><b>Non-exhaustive example:</b> Coaching pages or messages displayed to end users is cosmetically incorrect.</p>
"Software"	<p>means Specially Written Software, Supplier Software and Third-Party Software;</p>
"Source Code"	<p>means computer programs and/or data in eye-readable form and in such form that it can be compiled or interpreted into equivalent binary code together with all related design comments, flow charts, technical information and documentation necessary for the use, reproduction, maintenance, modification and enhancement of such software;</p>
"SSL"	<p>means Secure Sockets Layer;</p>



<b>"Supplier"</b>	means the United Net Connect <b>School-Secure</b> managed service for Primary schools owned and operated by United Network Technologies Limited, and as identified on the said Order Form;
<b>"Supplier Background IPR"</b>	means <ul style="list-style-type: none"><li>a) Intellectual Property Rights owned by the Supplier before the Commencement Date, for example those subsisting in the Supplier's or one of its software vendor's standard development tools, program components or standard code used in computer programming or in physical or electronic media containing the Supplier's Know-How or generic business methodologies; and/or</li><li>b) Intellectual Property Rights created by the Supplier independently of this Contract,</li></ul> but excluding Intellectual Property Rights owned by the Supplier subsisting in the Supplier Software;
<b>"Supplier Software"</b>	means any software which is proprietary to the Supplier (or an Affiliate or Reseller of the Supplier) and identified as such in the Order Form together with all other such software which is not identified in the Order Form but which is or will be used by the Supplier or any Reseller or Associate for the purposes of providing the Services or is embedded in and in respect of such other software as required to be licensed in order for the Customer to receive the benefit of and/or make use of the Services;
<b>"Supplier Solution"</b>	means the Supplier's solution being School-Secure managed service from United Net Connect;
<b>"Supplier System"</b>	means the information and communications technology system used by the Supplier in supplying the Services, including the Supplier Software, the Supplier Equipment, configuration and management utilities, calibration and testing tools and related cabling (but excludes the Customer System);
<b>"Technical Consultancy"</b>	means the provision of Supplier Personnel that are experienced cyber and data security resources, which may take the form of consultancy (at Customer premise and/or elsewhere) and / or training, or support for and access to information about the Services and may be ordered under this Contract at the prices set out in a United Network Technologies official quotation.



United Network Technologies is a specialist distributor for an extensive range of Cloud-only cyber security services and solutions into Commerce, Education and Public-sector markets which include many NHS Trusts, London Borough Councils, Legal Firms, Lloyds Insurance institutions and over 3,500 schools, colleges and universities.

<b>"Tender"</b>	a) means the tender submitted by the Supplier to an Authority, PSN, Local Authority or Trust;
<b>"Test" and "Testing"</b>	means any tests required to be carried out pursuant to this Contract as set out in the Test Plan or elsewhere in this Contract and <b>"Tested"</b> shall be construed accordingly;
<b>"Termination Notice"</b>	means a written notice of termination given by one Party to the other, notifying the Party receiving the notice of the intention of the Party giving the notice to terminate this Contract on a specified date and setting out the grounds for termination;
<b>"Third Party IPR"</b>	a) means Intellectual Property Rights owned by a third party but excluding Intellectual Property Rights owned by the third party subsisting in any Third Party Software;
<b>"Third Party Software"</b>	means any software identified as such in the Order Form together with all other software which is not listed in the Order Form which is proprietary to any third party (other than a Reseller Partner or Affiliate of the Supplier) or any Software which is or will be used by the Supplier for the purposes of providing the Services);
<b>"Threat Intelligence"</b>	a) means evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard;
<b>"Upgrade"</b>	means any patch, New Release or upgrade of Software and/or a Deliverable, including standard upgrades, product enhancements, and any modifications, but excluding any Update which the Supplier or a third party software supplier (or any Affiliate of the Supplier or any third party) releases during the Contract Period;
<b>"VAT"</b>	means value added tax in accordance with the provisions of the Value Added Tax Act 1994;
<b>"Virus"</b>	means a particular form of malware that uses computers to self-replicate and spread through software;
<b>"Whitelists"</b>	a whitelist is a list or register of entities that are being provided a particular privilege, service, mobility, access or recognition. Entities on the list will be accepted, approved and/or recognized. Whitelisting is the reverse of blacklisting, the

	practice of identifying entities that are denied, unrecognised, or ostracised;
<b>"Zero day malware"</b>	a) means a threat that exploits an unknown computer security vulnerability. The term is derived from the age of the exploit, which takes place before or on the first (or "zeroth") day of a developer's awareness of the exploit or bug. This means that there is no known security fix because developers are oblivious to the vulnerability or threat. Attackers exploit zero-day vulnerabilities through different vectors. Web browsers are the most common, due to their popularity. Attackers also send emails with attachments exploiting software attachment vulnerabilities.



## United Net Connect Managed Services - Technical Coverage, Support and Escalation Measures

### SCHEDULE - SERVICE LEVELS, SERVICE CREDITS AND PERFORMANCE MONITORING

United Network Technologies Limited or the School-Secure managed service from United Net Connect shall be referred in this document as the “Supplier”.

## 2. SCOPE

2.1 This Schedule (Service Levels, Service Credits and Performance Monitoring) sets out the Service Levels which the Supplier, United Net Connect, is required to achieve when providing Services, the mechanism by which Service Level Failures and Critical Service Level Failures will be managed and the method by which the Supplier's performance in the provision by it of these services will be so monitored.

2.2 This Schedule comprises:

- 2.2.1 (Part A) - Service Levels and Service Credits;
- 2.2.2 (Annex 1 to Part A) - Service Levels and Service Credits Table;
- 2.2.3 (Annex 2 to Part A) – Critical Service Level Failure;
- 2.2.4 (Part B) - Performance Monitoring; and
- 2.2.5 (Annex 1 to Part B) - Additional Performance Monitoring Requirements.
- 2.2.6 Team - Technical Team Members and Contact Information



United Network Technologies is a specialist distributor for an extensive range of Cloud-only cyber security services and solutions into Commerce, Education and Public-sector markets which include many NHS Trusts, London Borough Councils, Legal Firms, Lloyds Insurance institutions and over 3,500 schools, colleges and universities.



## **PART A: SERVICE LEVELS AND SERVICE CREDITS**

### **1. GENERAL PROVISIONS**

- 1.1 The Supplier shall provide a proactive Service Contract manager to ensure that all Service Levels in this Contract and Key Performance Indicators (KPI's) for the United Net Connect Service Agreement are achieved to the highest standard throughout.
- 1.2 The Supplier shall provide a managed service through the provision of a dedicated Contract manager where required on matters relating to:
  - 1.2.1 Availability;
  - 1.2.2 Latency;
  - 1.2.3 Incident Fix Times;
  - 1.2.4 Help Desk Call Answer;
  - 1.2.5 Participation in multi-supplier intervention;
  - 1.2.6 Problem Management; and
  - 1.2.7 Pupil, Teach, Staff Threat Detection Effectiveness.
- 1.3 The Supplier accepts and acknowledges that failure to meet the Service Level Performance Measures set out in the table in Annex 1 to this Part A of this Schedule will result in Service Credits being issued to its member schools.

### **2. PRINCIPAL POINTS**

- 2.1 The objectives of the Service Levels and Service Credits are to:
  - 2.1.1 ensure that the Offered Managed Service are of a consistently high quality and meet the requirements of each of its member schools;
  - 2.1.2 provide a mechanism whereby the school can attain meaningful recognition of inconvenience and/or loss resulting from the Supplier's failure to deliver the level of service for which it has contracted to deliver; and
  - 2.1.3 incentivise the Supplier to comply with and to expeditiously remedy any service failure to comply with the said Service Levels.

### **3. SERVICE LEVELS**

- 3.1 Annex 1 to this Part A of this Schedule sets out the Service Levels the performance of which the Parties have agreed to be measured.
- 3.2 The Supplier shall monitor its performance of this Contract by reference to the relevant performance criteria for achieving the Service Levels shown in Annex 1 to this Part A of



this Schedule and shall send the school a Performance Monitoring Report detailing the level of service which was achieved in accordance with the provisions of Part B (Performance Monitoring) of this Schedule.

3.3 The Supplier shall, at all times, provide the Services in such a manner that the Service Levels Performance Measures are achieved.

3.4 If the level of performance of the Supplier of any element of the provision but for the internet connection, by it of the Services during the Contract Period:

3.4.1 is likely to or fails to meet any Service Level Performance Measure or

3.4.2 is likely to cause or causes a Critical Service Failure to occur,

the Supplier shall immediately notify the school in writing, via email to the schools nominated person, and the school head teacher, in their absolute discretion and without prejudice to any other of its rights howsoever arising of this Contract (Service Levels and Service Credits), may:

- (a) require the Supplier to immediately take all remedial action that is reasonable to mitigate the impact on the school and to rectify or prevent a Service Level Failure or Critical Service Level Failure from taking place or recurring; and
- (b) if the action taken under paragraph (a) above has not already prevented or remedied the Service Level Failure or Critical Service Level Failure, the school shall be entitled to instruct the Supplier to comply with the Rectification Plan Process; or
- (c) if a Service Level Failure has occurred, deduct from the Contract Charges the applicable Service Level Credits payable by the Supplier to the school in accordance with the calculation formula set out in Annex 1 of this Part A of this Schedule; or
- (d) if a Critical Service Level Failure has occurred, exercise its right to Compensation for Critical Service Level Failure of this Contract (Critical Service Level Failure) (including subject, for the avoidance of doubt, the proviso in this Contract in relation to a Breach).

3.5 Approval and implementation by the school of any Rectification Plan shall not relieve the Supplier of any continuing responsibility to achieve the Service Levels, or remedy any failure to do so, and no waiver shall arise from any such Approval and/or implementation by the said school.

#### 4. SERVICE CREDITS

4.1 Annex 1 to this Part A of this Schedule sets out the formula used to calculate a Service Credit payable to the school as a result of a Service Level Failure in a given service period which, for the purpose of this Schedule, shall be a recurrent period of one Month during the Contract Period (the “**Service Period**”).

4.2 Annex 1 to this Part A of this Schedule includes details of each Service Credit available to each Service Level Performance Criterion if the applicable Service Level Performance



United Network Technologies is a specialist distributor for an extensive range of Cloud-only cyber security services and solutions into Commerce, Education and Public-sector markets which include many NHS Trusts, London Borough Councils, Legal Firms, Lloyds Insurance institutions and over 3,500 schools, colleges and universities.



Measure is not met by the Supplier. Service Credits shall be a percentage deduction from the Contract Charges for the relevant Service Period.

4.3 The school shall use the Performance Monitoring Reports supplied by the Supplier under Part B (Performance Monitoring) of this Schedule to verify the calculation and accuracy of all Service Credits, if any, applicable to each relevant Service Period.

4.4 Service Credits are a reduction of the amounts payable in respect of the Services and do not include VAT. The Supplier shall set-off the value of any Service Credits against the appropriate invoice issued upon reaching an anniversary date or Renewal date in accordance with calculation formula in Annex 1 of Part A of this Schedule.

## 5. NATURE OF SERVICE CREDITS

5.1 The Supplier confirms that it has modelled the Service Credits and has taken them into account in setting the level of the Contract Charges. Both Parties agree that the Service Credits are a reasonable method of price adjustment to reflect poor performance of the managed service should this occur.

## 6. SERVICE CREDIT CAP

6.1 For the purposes of this Contract the **Service Credit Cap** means for each Service Period. For the avoidance of doubt a Service Period is set at one year:

6.1.1 subject to paragraph 6.1.2, 10% of the Contract Charges payable to the school under this Contract in the Service Period immediately preceding the Month in respect of which Service Credits are accrued; and;

6.1.2 in any Service Period the Service Credit Cap shall be no more than 10% Service Credits.



United Network Technologies is a specialist distributor for an extensive range of Cloud-only cyber security services and solutions into Commerce, Education and Public-sector markets which include many NHS Trusts, London Borough Councils, Legal Firms, Lloyds Insurance institutions and over 3,500 schools, colleges and universities.

**ANNEX 1 TO PART A: SERVICE SEVERITY LEVELS AND SERVICE CREDITS TABLE**

**Table 1**

Severity Level Reference	Service Level Performance Criterion	Key Indicator	Service Level Severity Performance Measure	Service Credit for each Service Period (expressed as a percentage of the Contract Charges in respect of the Service Period to which the Service Credit relates)
1	Multi-supplier / Vendor intervention	EXAMPLE	The Supplier must attend Vendor intervention within 60 minutes at the request of the School.	Assigned Service Credit 1%
2	Help Desk Response Times	EXAMPLE	Percentage of calls answered within 15 minutes	Assigned Service Credit .75%
3	Availability of United Net Connect Service	EXAMPLE	At least 99.0% at all times.	Assigned Service Credit .5%
4	Service Incident Management	Help Desk - Call Answer  EXAMPLE	Details of Fix Time in respect of any Severity 4 Service Incident is no greater than 120 minutes.  > 180 minutes deemed a Service Level Failure	NO Service Credit(s) ASSIGNED 0%
5	Annual Performance	EXAMPLE	At least 99.9% at all times.  <99.5% deemed a Service Level Failure  This does not include Line connection	NO Service Credit(s) ASSIGNED 0%



## 1. ANNUAL PERFORMANCE AVAILABILITY MEASUREMENT

1.1 This Service Level shall apply to the United Net Connect Core Software-only Services and excludes any Internet Connection provided by any of the Wholesale Suppliers i.e. TalkTalk, Virgin, BT etc.

1.2 This Service Level shall be measured using the calculation set out below:

$$\text{Service Level \%} = ((\text{Total} - \text{To}) / \text{Total}) \times 100$$

To = the total duration (in minutes) of all periods where any aspect of the United Net Connect Software Services (excluding Line Connection) are not available within a Service Period.

Total = the total minutes within a Service Period.

1.3 For the avoidance of doubt, loss of availability shall be allowed for Permitted Software Maintenance or Upgrades, this is normally carried out overnight providing due warning to all member-schools.

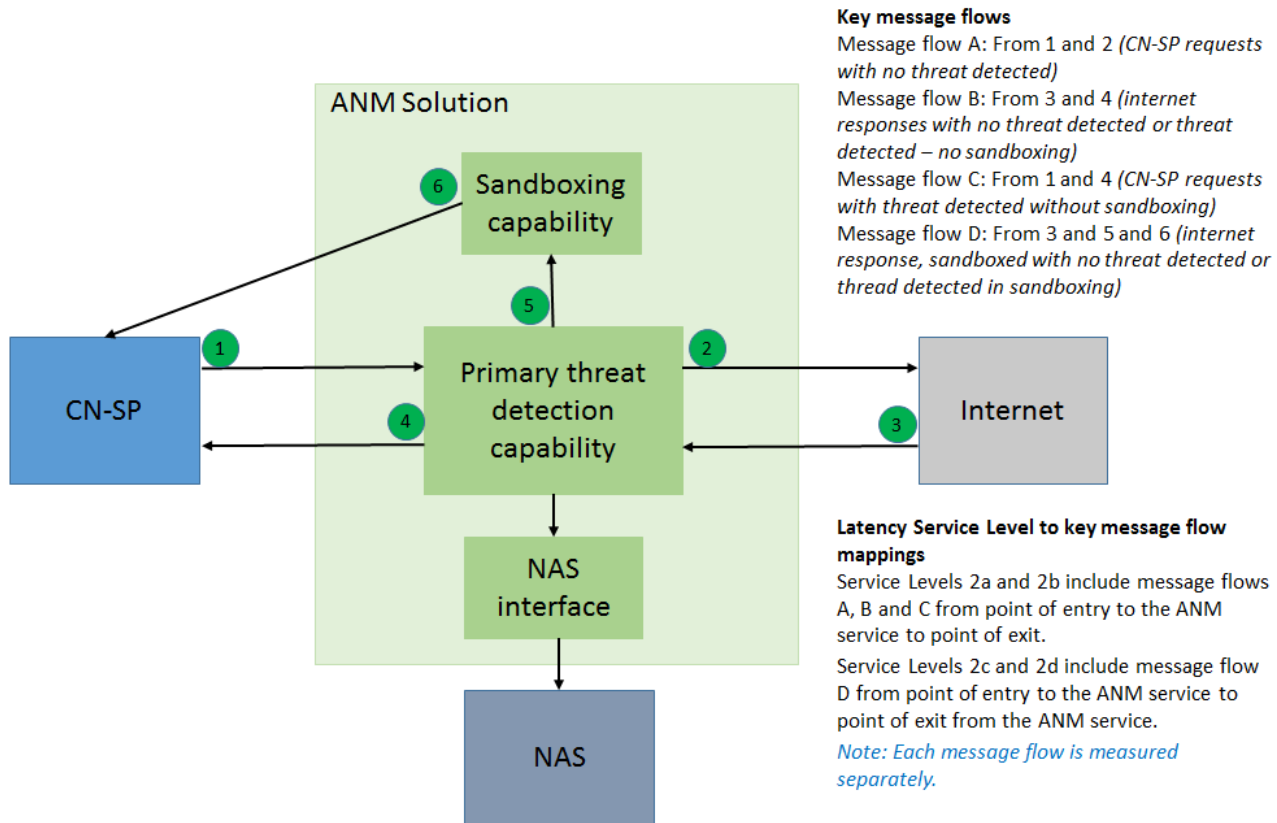
## 2. INTERNET CONNECTIVITY – PERFORMANCE – AVERAGE LATENCY

2.1 The illustration below sets out the key message flows through the ANM Core Services and their mapping to each of the Service Levels in the range 2a to 2d.



United Network Technologies is a specialist distributor for an extensive range of Cloud-only cyber security services and solutions into Commerce, Education and Public-sector markets which include many NHS Trusts, London Borough Councils, Legal Firms, Lloyds Insurance institutions and over 3,500 schools, colleges and universities.

## Logical representation of the key ANM message flows



2.2 Each of the message flows that map to each Service Level will be measured separately and taken into account in the performance against the Service Level.

2.3 With regard to Service Level References 2b and 2d the average latency across the worst performing 24-hour period will be measured on the following basis:

2.3.1 24 hour periods will be from 00.00 to 23:59 each day;

2.3.2 The latency of each message is measured as set out above;

2.3.3 The average over a 24-hour period is the sum of the latency of the messages over the 24-hour period divided by the sum of the number of messages over the 24-hour period.

2.4 Each message received from Primary schools during periods where demand exceeds the United Net Connect Service Capacity shall have any time spent queuing to be processed excluded from the measurement of Service Level Agreement.

### 3. INCIDENT MANAGEMENT – FIX TIME

3.1 The "**Fix Time**" of a Service Incident is the period from the time that the Service Incident has been reported to the Supplier, or has been identified by the Supplier's Performance Monitoring System, or that the Supplier becomes aware of the Service Incident by any other method, or the time at which the Supplier could reasonably have been expected to have identified it; to the point of its Resolution and "**Resolution**" means in relation to a Service Incident either:

3.1.1 the root cause of the Service Incident has been removed and the Services are being provided in accordance with the Service Requirements and Service Levels;  
or

3.1.2 the relevant Service User has been provided with a workaround in relation to the Service Incident, and the workaround has been accepted by the relevant Service User.

3.2 For the avoidance of doubt, where the Supplier was notified of a Service Incident via email or, via the Service web-portal, the Supplier shall be deemed to have been notified of the incident from the point the email or web-portal submission was received by the Supplier's Help Desk mailbox or web-portal tool, and not the point at which the Supplier logs the incident or responds to the submission.

3.3 Fix Times for all Service Incidents shall be measured in Operational Hours.

3.4 The Supplier shall measure 'Fix Times' as part of its service management responsibilities and report periodically to the school on Fix Times as part of the Performance Monitoring Report.

### 4. AVAILABILITY OF REPORTING FEED TO THE UNITED NET CONNECT SERVICE ANALYTICS TOOL

4.1 This Service Level shall be reported on the United Net Connect Reporting Software.

4.2 This Service Level shall be measured using the calculation set out below:

$$\text{Service Level \%} = ((\text{Total} - \text{To}) / \text{Total}) \times 100$$

To = the total duration (in minutes) of all periods where any aspect of the United Net Connect Service is not Available within a Service Period

Total = the total minutes within a Service Period

4.3 For the avoidance of doubt, no loss of Availability shall be allowed for Permitted Maintenance in school hours. This should be carried out outside of school hours unless otherwise agreed with each of the Head Teachers and/or Business Managers.



## 5. HELP DESK RESPONSE TIMES

- 5.1 Measurement of Service Level will be based on the time taken for a help desk operative to answer a call. Calls receiving an automated response or placed into a queuing system shall be deemed not to have been answered. The Supplier shall monitor the support response times and shall provide the results of such monitoring to the school as part of the Monthly Performance Monitoring Report.
- 5.2 The measure for the Service Level starts when the call is recognised by the Supplier's telephony system and ends when the call is answered by a help desk operative.
- 5.3 Quarterly statistical analysis will be provided relating to each school relating to bullying, malware attack, radicalisation etc. This information will be reported on a per child basis.
- 5.4 Should the bullying, malware attack or radicalisation be deemed of an urgent nature then a member of the Service provider will inform the designated person in the school and provide such evidence.

## 6. MULTI SUPPLIER INTERVENTION

- 6.1 Upon request from the school's safeguarding person or from a Head teacher, the Supplier shall, within 2 days, attend and contribute to a multi supplier intervention or meeting.

## 7. PROBLEM MANAGEMENT RESOLUTION

- 7.1 Subject to paragraph 7.2 below, the "**Problem Resolution Time**" in respect of a Problem is the period from the time that the associated Service Incident has reached a Resolution to the point at which a Permanent Fix has been reached.
- 7.2 Where one or more Service Incidents are associated with a Problem already identified by a separate Service Incident, the Problem Resolution Time shall be deemed to start upon the earliest Resolution of any of those Service Incidents.
- 7.3 The Problem Management Resolution Service Level Performance Criterion measures the time taken to resolve Problems dependent on the Severity Level the Problem has been allocated.
- 7.4 A Problem shall only be deemed as resolved when all Service Components impacted by the relevant Problem have received a Permanent Fix and the School confirms acceptance to the Supplier.
- 7.5 Upon request, the Supplier shall update the school about any aspects of a Problem.
- 7.6 Where the Problem Resolution Time exceeds the Service Level Performance Measure, a Service Credit shall accrue for the associated Service Period and for each subsequent Service Period(s) until a Permanent Fix has been reached.



United Network Technologies is a specialist distributor for an extensive range of Cloud-only cyber security services and solutions into Commerce, Education and Public-sector markets which include many NHS Trusts, London Borough Councils, Legal Firms, Lloyds Insurance institutions and over 3,500 schools, colleges and universities.



7.7 If, after the Supplier has measured the Problem Resolution Time for a Problem it is later established, that the Supplier did not originally resolve the Problem; or the Problem reoccurs within 10 days of the Problem being resolved, the Problem shall be deemed not to have been resolved in the first place and, in which case, the measurement of the Problem Resolution Time shall:

7.7.1 be deemed to be ongoing until the Problem is resolved; and

7.7.2 include the time period that the Problem was temporarily resolved and/or the time period that the Supplier believed that the Problem was resolved.

## 8. PUPIL, TEACHER, STAFF THREAT DETECTION EFFECTIVENESS

8.1 The school shall have the option, at its sole discretion, to arrange and carry out a physical Threat Detection Effectiveness Test each Service Period. For the avoidance of doubt, the full test (including both executions) shall be carried out no more than once per Service Period (per year).

8.2 The Threat Detection Effectiveness Test, which ranges from bullying tactics, radicalisation techniques, malware and email attack interventions, shall consist of a range of interactions with the United Net Connect services team with the objective of identifying the extent to which threats are identified and dealt with. These Tests will consist of various emails (via port 80), web portal access (via port 443) to test the effectiveness of protection provided for pupils, teachers and staff.

8.3 Regardless of the pass or fail outcome agreed for the Threat Detection Effectiveness Tests, the Supplier shall, wherever practicable and by agreement with the school, update the United Net Connect services team to enhance the threat detection capability to address any shortfalls in the effectiveness of the threat identification / prevention determined by the Threat Detection Effectiveness Tests and shall keep the School informed of progress in the execution of those updates via the Head teacher or appointed Safeguarding officer.

## 9. UNUSED SECTION – THREAT DETECTION, SANDBOX CONTAINERISATION AND FURTHER REMEDIATION

PLEASE DO NOT USE – THIS SECTION DOES NOT APPLY TO PRIMARY SCHOOLS



## ANNEX 2 TO PART A: CRITICAL SERVICE LEVEL FAILURE

1. A Critical Service Level Failure shall mean either:
  - a. the Supplier accruing Service Credits to a value of 10% (or higher) of the Contract Charges in a Service Period (ignoring the Service Credit Cap); or
  - b. 5 or more Major Service Level Failures accumulated in a Service Period (a year).
2. The number of Service Level Performance Criteria in relation to which the School may, on giving the Supplier at least 3 Months' notice, change the Service Level Performance Measure and/or Service Credit allocation pursuant to Clause 13.6.1 shall be 2.

## ANNEX 2 TO PART B: PERFORMANCE MONITORING

### 1. PRINCIPAL POINTS

- 1.1 Part B to this Schedule provides the methodology for monitoring the provision of the Services:
  - 1.1.1 to ensure that the Supplier is complying with the Service Levels; and
  - 1.1.2 for identifying any failures to achieve Service Levels in the performance of the Supplier and/or provision of the Services ("Performance Monitoring System").
- 1.2 Within twenty (20) Working Days of the Commencement Date the Supplier shall provide the school with details of how the process in respect of the monitoring and reporting of Service Levels will operate between the Parties and the Parties will endeavour to agree such process as soon as reasonably possible.

### 2. REPORTING OF SERVICE FAILURES

- 2.1 The Supplier shall report all failures to achieve Service Levels and any Critical Service Level Failure to the school in accordance with the processes agreed in paragraph 1.2 of Part B of this Schedule above.

### 3. PERFORMANCE MONITORING AND PERFORMANCE REVIEW

- 3.1 Unless otherwise requested by the school, the Supplier shall provide the school with performance monitoring reports ("**Performance Monitoring Reports**") within 10 Working Days of the end of each Service Period in accordance with the process and timescales agreed pursuant to paragraph 1.2 of Part B of this Schedule above which shall contain, as a minimum, the following information in respect of the relevant Service Period just ended and achieved over the previous Service Period where applicable;



United Network Technologies is a specialist distributor for an extensive range of Cloud-only cyber security services and solutions into Commerce, Education and Public-sector markets which include many NHS Trusts, London Borough Councils, Legal Firms, Lloyds Insurance institutions and over 3,500 schools, colleges and universities.



- 3.1.1 for each Service Level, the actual performance achieved over the Service Level for the relevant Service Period;
- 3.1.2 a summary of all failures to achieve Service Levels that occurred during that Service Period, which shall include:
  - (a) details of each Service Level failure which occurred during the Service Period, where applicable ordered by Severity Level; and
  - (b) which performance failures remain outstanding and progress in resolving them;
    - 3.1.3 details of any Service Level Failures which occurred during the Service Period;
    - 3.1.4 any Critical Service Level Failures and details in relation thereto;
    - 3.1.5 for any repeat failures, actions taken to resolve the underlying cause and prevent recurrence;
    - 3.1.6 the Service Credits to be applied in respect of the relevant period indicating the failures and Service Levels to which the Service Credits relate; and
    - 3.1.7 such other details as the school may reasonably require from time to time.
- 3.2 The Parties shall attend meetings to discuss Performance Monitoring Reports ("**Performance Review Meetings**") on an annual basis (unless otherwise agreed). The Performance Review Meetings will be the forum for the review by the Supplier and the school of the Performance Monitoring Reports. The Performance Review Meetings shall (unless otherwise agreed):
  - 3.2.1 take place within 5 working days of the Performance Monitoring Reports being issued by the Supplier upon reaching the end of a Service period (a year);
  - 3.2.2 take place at such location and time (within normal business hours) as the school shall reasonably require unless otherwise agreed in advance;
  - 3.2.3 be attended by the Supplier's Representative and the school's Representative;
- 3.3 The school shall be entitled to raise any additional questions and/or request any further information regarding any failure to achieve Service Levels.
- 3.4 The Supplier shall provide to the school such supporting documentation as the school may reasonably require in order to verify the level of the performance by the Supplier and the calculations of the amount of Service Credits for any specified Service Period.

#### 4. SATISFACTION SURVEYS

- 4.1 In order to assess the level of performance of the Supplier, the school or schools may undertake satisfaction surveys in respect of the Supplier's provision of the Services.



United Network Technologies is a specialist distributor for an extensive range of Cloud-only cyber security services and solutions into Commerce, Education and Public-sector markets which include many NHS Trusts, London Borough Councils, Legal Firms, Lloyds Insurance institutions and over 3,500 schools, colleges and universities.



- 4.2 The school shall be entitled to notify the Supplier of any aspects of their performance of the provision of the Services which the responses to the Satisfaction Surveys reasonably suggest are not in accordance with this Contract.
- 4.3 All other suggestions for improvements to the provision of Services shall be dealt with as part of the continuous improvement programme pursuant to Clause 4.



United Network Technologies is a specialist distributor for an extensive range of Cloud-only cyber security services and solutions into Commerce, Education and Public-sector markets which include many NHS Trusts, London Borough Councils, Legal Firms, Lloyds Insurance institutions and over 3,500 schools, colleges and universities.



## ANNEX 1 TO PART B: ADDITIONAL PERFORMANCE MONITORING REQUIREMENTS

In this Schedule, the following definitions shall apply:

- "Senior Service Manager"** means the manager described in paragraph 5.1 of this Annex;
- "Technical Service Board"** means the board described in paragraph 5.1 of this Annex;

### 5. MANAGEMENT OF THE SERVICES

- 5.1 The Supplier and the school shall each appoint a Senior Service Manager for the purposes of this Contract through whom the provision of the Services shall be managed on a day-to-day basis. For a primary school it is normal practice to appoint the Safeguarding officer.
- 5.2 Both parties shall ensure that appropriate resource is made available on a regular basis including, for example, a Technical Service Board such that the aims, objectives and specific provisions of this Contract can be fully realised.

### 6. TECHNICAL SERVICES BOARD FOR THE UNITED NET CONNECT MANAGED SERVICE

- 6.1 The Technical Service Board shall be established by member schools in accordance with the Supplier, for the purposes of this Contract on which the Supplier and member schools shall be duly represented.
- 6.2 Each school shall receive a list of the Technical Service Board members, frequency and location of board meetings and next date at which the board shall convene. For which each member school shall be given 30 days' notice thereof.
- 6.3 In the event that any member school wishes to replace any of its appointed board members, that party shall notify the other in writing of the proposed change for agreement by the other Party (such agreement not to be unreasonably withheld or delayed).
- 6.4 Each Party shall ensure that its board member shall make all reasonable efforts to attend board meetings at which that board member's attendance is required. If any board member is not able to attend a board meeting, that person shall use all reasonable endeavours to ensure that a delegate attends in his/her place (wherever possible) is properly briefed and prepared and that he/she is debriefed by such delegate after the board meeting.
- 6.5 The Technical Service Board shall be accountable to member schools for the technology used by the Supplier and ensuring that technological choices are made to maximise the long term value of all Services provided through the United Net Connect Managed Service.
- 6.6 The Technical Service Board shall:



United Network Technologies is a specialist distributor for an extensive range of Cloud-only cyber security services and solutions into Commerce, Education and Public-sector markets which include many NHS Trusts, London Borough Councils, Legal Firms, Lloyds Insurance institutions and over 3,500 schools, colleges and universities.



- 6.6.1 assure compliance with the overall technical architecture of the school and to Home Office compliance and adhering to IWF Guidelines (as defined at [www.unitednetconnect.com](http://www.unitednetconnect.com));
- 6.6.2 grant dispensations for variations from such compliance where appropriate;
- 6.6.3 assure the coherence and consistency of the software architecture for the provision of the Services;
- 6.6.4 monitor developments in new technology and reporting on their potential benefit to the provision of the United Net Connect Managed Service;
- 6.6.5 provide advice, guidance and information on technical issues; and assure that the technical architecture for the provision of the Services is aligned to the requirements of Primary schools and has sufficient flexibility to cope with future requirements of any of its member schools.



United Network Technologies is a specialist distributor for an extensive range of Cloud-only cyber security services and solutions into Commerce, Education and Public-sector markets which include many NHS Trusts, London Borough Councils, Legal Firms, Lloyds Insurance institutions and over 3,500 schools, colleges and universities.