

As an IoT company, QIoT Ltd aim to support your healthcare objectives. To do so, we may collect your personal data to provide you with our services unless you are a patient of the NHS or Private Healthcare Company where we may not record any Personal Identifiable Information (PII). We do not take your trust for granted so we've developed a Privacy Policy that covers how we collect, use, disclose, transfer, and store your personal data.

This Privacy Policy was last updated in June 2021.

Who We Are

This General Privacy Policy ("Privacy Policy") applies to the QIoT Ltd and any related companies (collectively "we," "us" or "our").

If you live in the [European Economic Area](#), the Controller of your personal data is QIoT Ltd, which has its principal place of business at Unit 260, Embroidery Mill, AbbeyMill Business Centre, Paisley, Scotland PA1 1TJ.

Privacy Policy Contents

This Privacy Policy describes how we handle and protect your personal data and the choices available to you regarding collection, process, access, and how to update, correct and delete your personal data. Additional information on our personal data practices may be provided in product settings, contractual terms, or notices provided prior to or at the time of data collection.

This Privacy Policy is intended for you if you are a user of our products and services.

Personal Data We Process

Personal data refers to any information relating to an identified or identifiable natural person ("Personal Data").

We may collect data or ask you to provide certain data when you visit and use our websites, products and services. The sources from which we collect Personal Data include:

- Data collected directly from you or your device relating to an identified or identifiable natural person ("Data Subject"), and may include direct identifiers such as name, address, email address, phone number, and online or indirect identifiers such as CHI number, Password, Device Identifiers, Device Usage identifiers, or IP address;
- We are unlikely to need to invoice you for the device or reporting unless you come to us directly, in which case we will also collect billing data.
- If we link other data relating to you with your Personal Data, we will treat that linked data as Personal Data; and
- We may also collect Personal Data from trusted third-party sources such as NHS systems.

We do not process special categories of personal data or deduce in any way this type of information from data we collect within our products.

We organize the Personal Data we process into these basic categories: Billing Data, Account Data, and Product Usage Data.

Billing Data includes your name, email address, and your phone number. In most circumstances, you purchase our products and services directly from ourselves, **but we may use a trusted third-party service provider, reseller, or app store.** In those circumstances, your Billing Data is processed by the relevant third party and we only receive a subset of this data to keep proper business records. In these instances, see below an example of Billing Data and what we use it for:

Billing data	What we use it for
Email address	To send you purchase receipts
Renewability	To check if a given subscription can be renewed
Date of expiry	To check whether a license is valid

Account Data includes information needed to set up and customize an account, such as your name, email address and username, and information connected with our services, such as license keys. For some of our products or some of their functions creating an account is necessary. See below an example of Account Data and what we use it for:

Account data	What we use it for
Name	To customize our communications by addressing you by your name
Email address	To send you communications regarding your license and support
Username	To manage your account and facilitate your login into the service
Subscription renewal date	To tell us until when the account is valid
Trial User	To add a trial period before the account is charged

Product Data includes two sub-categories:

- **Device Data** includes information about the device number; and
- **Service Data** includes information about the QIoT product usage and events relating to use of our product by you such as date and time of usage.

Why We Process Your Personal Data

We use your Personal Data for the following purposes and on the following grounds:

On the basis of fulfilling our contract with your healthcare provider or entering into a contract with you on your request, in order to:

- Keep our products or services up-to-date, safe and free of errors, including implementation of new product features and versions;
- Provision the download, activation, and performance of the product or service;
- Verify your identity and entitlement to paid products or services, when you contact us for support or access our services;
- Process your purchase transactions;
- Provide you with technical and customer support.
- Update you on the status of your orders and licences;
- Process purchase of our products or services from us;
- Manage your subscriptions and user accounts; and

We will always ask for your consent before any processing that requires it and provide you with necessary information.

On the basis of legal obligations, we process your Personal Data when it is necessary for compliance with a legal tax, accounting, anti-money laundering, legal order, sanction checks or other obligation to which we are subject.

On the basis of our legitimate interest we will use your Personal Data to:

- Communicate about possible security, privacy and performance improvements and products that supplement or improve our purchased products and to optimize the content and delivery of this type of communication;
- Evaluate and improve the performance and quality of our products, services and websites, develop new products, train our employees and to understand usage trends, and analyse user acquisitions, conversions and campaigns;
- Allow interoperability within our applications;
- Secure our systems and applications;
- Allow effective performance of our business by ensuring necessary internal administrative and commercial processes (e.g. finances, controlling, business intelligence, legal & compliance, information security etc.); and
- Establish, exercise or defend our legal rights.

For the above-mentioned processing operations, we have balanced your interests against our interests. In any case, you have the right to object, on grounds relating to our particular situation, to those processing operations.

Balancing Legitimate Interests

Before relying on our legitimate interests, we balanced them against your interests and made sure they are compelling enough and will not cause any unwarranted harm. With respect to the purposes below we consider necessary to explain what our interests are in detail.

Systems, Apps and Network Security

We process Personal Data for network and information security purposes. In line with EU data protection law, organizations have a recognized legitimate interest in collecting and processing Personal Data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security. This primarily covers the ability of a network or of an information system to resist events, attacks or unlawful or malicious actions that could compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, or the security of the related services offered by, or accessible via those networks and systems.

Both as an organization in our own right, and as a provider of cybersecurity technologies and services which may include hosted and managed cybersecurity technology services, it is necessary for the functionality of our systems, products and services and in our legitimate interests as well as in our users', to collect and process Personal Data to the extent strictly necessary and proportionate for the purposes of ensuring the security of our own, and of our users' networks, devices, and information systems. This includes the development of threat intelligence resources aimed at maintaining and improving on an ongoing basis the ability of our networks and systems, and those of certain partners, to resist unlawful or malicious actions and other harmful events ("cyber-threats").

The Personal Data we process for said purposes includes, without limitation, network traffic data related to cyber-threats such as:

- Device usage data);
- Device location data at time of usage;
- Atmospheric conditions at place and time of device usage.

Depending on the context in which such data is collected, it may contain Personal Data concerning you or any other Data Subjects. However, in such cases, we will process the data concerned only to the extent strictly necessary and proportionate to the purposes of detecting, blocking, reporting (by removing any personally identifiable elements) and mitigating the cyber-threats of concern to you, and to secure your network, device and systems. When processing Personal Data in this context, we do not seek to identify a Data Subject.

Product and business improvement

We have a legitimate interest to use necessary Personal Data to understand user conversions, acquisitions and campaign performance through various distribution channels, and users' download, activation and interactions with our products because these analytics help us improve functionality, effectiveness, security and reliability of our products and business activities and develop new products. This processing may include using third-party tools.

How We Process Your Personal Data

We do our best to disconnect or remove all direct identifiers from the Personal Data that we use:

- removal of identifiers begins when the products and services are initially activated. For paid users we keep Billing Data in a separate database and minimize its use for anything other than handling payments and our own finances.
- we continuously monitor for, minimize, disconnect, and remove all direct identifiers during the normal performance of the products and services.

Personalization

We may use your answers from surveys, in which you can participate, and relevant Product Data to personalize communication and recommend our relevant products for you.

We do not take any decisions solely based on algorithms, including profiling, that would significantly affect you.

How We Disclose Your Personal Data

We only disclose your Personal Data as described below, within our group, with our partners, with service providers that provide your primary healthcare, or as required by applicable law. Processing is only undertaken for the purposes described in this Privacy Policy. If we disclose your Personal Data, we require its recipients to comply with adequate privacy and confidentiality requirements, and security standards.

Payment processors

If you opt to pay for use of our services, we will use a third-party payment processor to take payment from you. These third parties are properly regulated and authorized to handle your payment information and are prohibited from using your Personal Data for any other purposes other than arranging these services for us. However, they are independent controllers of your data with their own responsibility.

These are our long-term payment processors:

Payment Processor	Link to Privacy Policy	Location
Bank of Scotland	https://www.bankofscotland.co.uk/insurance/privacy-policy.html	UK & Ireland
Paypal	https://www.paypal.com/en/webapps/mpp/ua/privacy-full	US, Ireland
Google Play Store (for mobile apps)	https://policies.google.com/privacy	US, Ireland
Apple Store (for mobile apps)	https://www.apple.com/legal/privacy/	US, Ireland

Your Billing Data is processed by the payment processor from whom you purchased the product. Your data is processed according to the relevant processor's privacy policy.

Service Providers

We may use contractors and service providers to process your Personal Data for the purposes described in this Privacy Policy. We contractually require service providers to keep data secure and confidential. Such service providers may include in particular, professional consultants.

Sometimes these service providers will be independent controllers of your data and their terms and conditions, end user license agreements (“EULA”) and privacy statements will apply to such relationships.

Distributors, Resellers

We may provide your Personal Data to our partners for the purpose of distribution, sale or management of our products. Our partners may use your Personal Data to communicate with you and others about QIoT products or services. In addition, you purchase our products directly from our distributor, a reseller, or an app store. Because your relationship in these cases is with that distributor, reseller or an app store, such third party will also process your Personal Data.

Analytics Tool Providers

We use analytical tools, including third-party analytical tools, which allow us to, among other things, identify potential performance or security issues with our products, improve their stability and function, understand how you use our products, and websites, so that we can optimize and improve your user experience, as well as evaluate and improve our campaigns. We use Service and Device data for analytics.

Below, we list these partners and tools and their privacy policies.

Tool (provider)	Type of Analytics	Link to Privacy Policy	Location
Google Analytics (Google)	user behaviour	https://support.google.com/analytics/answer/6004245 https://policies.google.com/privacy https://support.google.com/analytics/answer/6366371?hl=en&ref_topic=2919631	US, Ireland
Firebase Analytics (Google)	user behaviour (advanced features like A/B testing, predictions)	https://firebase.google.com/support/privacy/ https://policies.google.com/privacy	US, Ireland
AppsFlyer (AppsFlyer)	user acquisition	https://www.appsflyer.com/privacy-policy/	Germany
Adjust (Adjust)	user acquisition	https://www.adjust.com/terms/privacy-policy/	Germany
ZUDU	App Development	https://zudu.co.uk/	UK

--	--	--	--

Please note that not all of our products use all of these third-party analytics tools. Analytics tools that we use for diagnosing your product are necessary for service provision.

Public Authorities

In certain instances, it may be necessary for us to disclose your Personal Data to public authorities or as otherwise required by applicable law. No Personal Data will be disclosed to any public authority except in response to:

- A subpoena, warrant or other process issued by a court or other public authority of competent jurisdiction;
- A legal process having the same consequence as a court-issued request for data, in that if we were to refuse to provide such data, it would be in breach of local law, and it or its officers, executives or employees would be subject to liability for failing to honor such legal process;
- Where such disclosure is necessary for us to enforce its legal rights pursuant to applicable law; or
- A request for data with the purpose of identifying and/or preventing credit card fraud.

Mergers, Acquisitions and Corporate Restructurings

Like any other company, we too go through its own cycle of growth, expansion, streamlining and optimization. Its business decisions and market developments therefore affect its structure. As a result of such transactions, and for maintaining a continued relationship with you, we may transfer your Personal Data to a related affiliate.

If we are involved in a reorganization, merger, acquisition or sale of our assets, your Personal Data may be transferred as part of that transaction. We do not need to notify you of any such deal, when applicable.

How We Protect Your Personal Data

We maintain administrative, technical, and physical safeguards for the protection of your Personal Data.

Administrative Safeguards

Access to the Personal Data of our users is limited to authorized personnel who have a legitimate need to know based on their job descriptions, for example, employees who provide technical support to end users, or who service user accounts. In the case of third-party contractors who process personal information on our behalf, similar requirements are imposed. These third parties are contractually bound by confidentiality clauses, even when they leave. Where an individual employee no longer requires access, that individual's credentials are revoked.

Technical Safeguards

We store your personal information in our database using the protections described above. In addition, we utilize up-to-date [firewall](#) protection for an additional layer of security. We use high-quality antivirus and [anti-malware](#) software, and regularly update our [virus](#) definitions. Third parties who we hire to provide services and who have access to our users' data are required to implement privacy and security practices that we deem adequate.

Physical Safeguards

Access to user information in our database by Internet requires using an encrypted VPN, except for email which requires user authentication. Otherwise, access is limited to our physical premises. Physical removal of Personal Data from our location is forbidden. Third-party contractors who process Personal Data on our behalf agree to provide reasonable physical safeguards.

Proportionality

We strive to collect no more Personal Data from you than is required by the purpose for which we collect it. This, in turn, helps reduce the total risk of harm should data loss or a breach in security occur: the less data we collect, the smaller the overall risk.

How Long We Store Your Personal Data

We will hold your Personal Data on our systems for the following periods:

- For Product Data, only as long as necessary for the purposes of a particular product or service. We use rolling deletion periods which means we regularly delete collected data in the given periods starting from the collection of that respective data. **The rolling deletion periods for Product Data are not longer than twelve years..** Please note that when you uninstall our product, processing for service provision, analytics, if applicable, dependent on the installed product shall cease. **After the uninstallation, we will continue to process your Product Data for statistical purposes for up to twelve years,** however, we have appropriate measures in place, including pseudonymization.
- For Billing Data, for as long as we have a legal obligation or for our legitimate interests in establishing legal rights;
- For Account Data, for as long as you maintain your account;

Storage of Your Personal Data

The data we collect from you may be stored, with risk-appropriate technical and organizational security measures applied to it, on in-house as well as third-party servers in the in the UK and/or United States, as well as anywhere we or our trusted service providers and partners operate.

In all cases, we follow generally accepted standards and security measures to protect the personal data submitted to us, both during transmission and once we receive it.

Your Privacy Rights

You have the following rights regarding the processing of your Personal Data:

- Right to information - Right to receive information about the processing of your Personal Data, prior to processing as well as during the processing, upon request.
- Right of access - Aside from the information about the processing of your Personal Data, you have the right to receive a copy of your Personal Data undergoing processing.
- Right to rectification - We should process accurate Personal Data; if you discover inaccuracy, you have the right to seek rectification of inaccurate Personal Data.
- Right to erasure ("right to be forgotten") - You have the right to erasure of your Personal Data, but only in specific cases stipulated by law, e.g., if there is no legally recognized title on our part for further processing of your Personal Data (incl. protection of QIoT's legitimate interests and rights).
- Right to data portability - The right to receive Personal Data which you have provided and is being processed on the basis of consent or where it is necessary for the purpose of conclusion and performance of a contract, in machine-readable format. This right applies exclusively to Personal Data which processing is carried out by automated means.
- Right to object - Applies to cases of processing carried out in legitimate interest. You have the right to object to such processing, on grounds relating to your particular situation, and we are required to assess the processing in order to ensure compliance with all legally binding rules and applicable regulations. In case of direct marketing, we shall cease processing Personal Data for such purposes after the objection.
- Right to withdraw consent - In the case of processing based on your consent, you can withdraw your consent at any time, by using the same method (if technically possible) you used to provide it to us (the exact method will be described in more detail with each consent when you provide it). The withdrawal of consent shall not affect the lawfulness of processing based on your consent before its withdrawal.
- Right to restriction of processing - You have the right to restriction of processing of your Personal Data if: You are contesting the accuracy of your Personal Data, for a period enabling us to verify the accuracy of your Personal Data; the processing is unlawful and you oppose the erasure of the Personal Data and request the restriction of its use instead; we no longer need the Personal Data for the purposes of the processing, but they are required by you for the establishment, exercise or defence of legal claims; or you have objected to processing of your Personal Data, and there is a pending verification whether our legitimate grounds override your interests.
- Right to contact supervisory authority, court - You may contact and lodge a complaint with the supervisory authority – The Office for Personal Data Protection or your local authority or a relevant court.

The fulfilment of data subject rights listed above will depend on the category of Personal Data and the processing activity. In all cases, we strive to fulfil your request.

We will action your request within one month of receiving a request from you concerning any one of your rights as a Data Subject. Should we be inundated with requests or particularly complicated requests, the time limit may be extended to a maximum of another two months. If we fail to meet these deadlines, we would, of course, prefer that you contact us to resolve the situation informally.

Where requests we receive are manifestly unfounded or excessive, in particular because of their repetitive character, we may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (b) refuse to act on the request.

Contact Us

To exercise any of your rights, or if you have any other questions or complaints about our use of your Personal Data and its privacy, write our Privacy Team through the most convenient channel below:

We are registered as QIoT Ltd and our registered address is Unit 260, Embroidery Mill AbbeyMill Business Centre, Paisley, Scotland PA1 1TJ info@qiot.co.uk customerservices@qiot.co.uk Please type "PRIVACY REQUEST" in the message line of your email so we can have the appropriate member of the QIoT team respond.

If you prefer, you can send paper mail to QIoT Ltd Unit 260, Embroidery Mill, AbbeyMill Business Centre, Paisley, Scotland PA1 1TJ. Be sure to write "Attention: PRIVACY" in the address so we know where to direct your correspondence.

Data Protection Officer

As required under the GDPR, we have a data protection officer (DPO) to monitor our compliance with the GDPR, provide advice where requested and cooperate with supervisory authorities. You can contact our data protection officer via info@qiot.co.uk. Please type "Data Protection officer" in the message line of your email so we can have the appropriate member of the QIoT team respond.

Changes to this Privacy Policy

We reserve the right to revise or modify this Privacy Policy. In addition, we may update this Privacy Policy to reflect changes to our data practices. If we make any material changes, we will notify you by email (sent to the e-mail address specified in your account) or by means of a notice on this website prior to the change becoming effective. We encourage you to periodically review this page for the latest information on our privacy practices.

Privacy Policy Payment Terms & Conditions.

Terms Used in this Agreement:

1.1 "Agreement" means these terms and conditions, the Order Form, and the Tariff.

1.2 "Airtime" means airtime and network capacity procured from the Network Operator.

1.3 "End-User Licensed Software" (EUL) means any software, the licence terms for which are governed by a separate agreement with the licensor of such software typically by means of a "click-wrap" or "shrink-wrap" licence agreement.

1.4 "Equipment" means the items supplied by us under this Agreement and includes any Software (but not End-User Licensed Software) and documentation supplied under this agreement.

1.5 "Gateways" are devices that transfer data onto a radio network via a SIM card and radio channel, thus gaining a mobile-mobile call rate rather than fixed-mobile.

1.6 "GPRS Bearer" means the General Packet Radio Service provided by the Network Operator that forms part of the Airtime.

1.7 "Mobile device" means the mobile equipment incorporating a SIM card.

1.8 Mobile Web is full colour Internet access and email on the move.

1.9 "Network" is the QIoT Remote Monitoring Network over which our services are provided. This is a digital network, which works in many countries and may allow you to use your QIoT Remote Monitoring in those countries.

1.10 "Network Operator" means the network operator who operates the network of networks to which the SIM Cards are connected.

1.11 "Order Form" means the QIoT Ltd order form to which these terms and conditions are attached, and which contain details of your application for the Service and the QIoT Remote Monitoring.

1.12 "Service" means the provision of Airtime, Equipment, GPRS Bearer, Mobile Web, SMS, SMS Land to Mobile Text Messaging Service, location-based services and/or any other Services.

1.13 "Software" means any software (excluding End User Licensed Software) supplied to the Customer by your QIoT, under the terms of or in respect of this Agreement.

1.14 "SIM Card" means the subscriber identity module supplied by your Network Operator (and which shall at all times remain the property of the Network Operator), which is utilised by you to receive the service.

1.15 "SMS" means the short message service, which enables text messages to be sent to, and received from Devices.

1.16 "SMS Land to Mobile Text Messaging Service" means the short message service for text message sent to SIM Cards via a software application in conjunction with a private or virtual private circuit linking the Customer's private or virtual private data network with the Services.

1.17 "QIoT Ltd" or "we, us" means QIoT Ltd of Unit 260 Embroidery Mills, Abbey Mills Paisley PA11TJ.

1.18 "Tariff" means the QIoT Ltd tariff that sets out the rates, which we will charge you for our service that you have chosen. Please contact us if you have not received a copy of our Tariff with the Order Form.

1.19 "Term" the length of time you commit to taking the Service for each QIoT Remote Monitoring or QIoT Remote Monitoring upgrade ordered as more particularly described in Clause 3. The initial Term is specified on the Order Form under the Length of Agreement.

1.20 "You" means the customer whose company details or personal details are set out on the Order Form

2. Scope of the Agreement:

2.1 QIoT Ltd agrees to provide you with the Service and/or QIoT Remote Monitoring and you agree to use the Service and the QIoT Remote Monitoring on the terms set out in this Agreement.

2.2 This agreement and any other document referred to herein sets out the entire agreement between us relating to any QIoT Remote Monitoring or Service supplied to you by QIoT Ltd. You acknowledge that you have not relied on any representation, undertaking,

3. Length of Agreement:

3.1 This Agreement begins when we either accept your application for the Service and/or QIoT Remote Monitoring in writing or when we send you access to the QIoT Remote Monitoring Service you have ordered, whichever is the earlier. Our acceptance of your application is subject to your passing a UK credit check, your consent to our submitting your details to a credit reference agency for this purpose and by signing this Agreement.

3.2 You agree that each QIoT Remote Monitoring ordered by you is subject to its own agreement. The Term commences on the date of initial connection of your QIoT Remote Monitoring Service. The initial Term is specified on the Order Form under Length of Agreement. The Term shall automatically be extended until written notice is given to terminate under clause 8.3.

3.3 Upgrades: If you upgrade your QIoT Remote Monitoring to a new model, then the new model will be subject to a new Term from the date the new model was delivered.

4. Supply of QIoT Remote Monitoring:

4.1 We will try to deliver the QIoT Remote Monitoring within agreed timescales, under no circumstances shall we be liable to you for any loss of any kind whatsoever caused by any delay in delivery of the QIoT Remote Monitoring.

4.2 QIoT Ltd is not the manufacturer of any QIoT Remote Monitoring supplied to you under this Agreement. QIoT Ltd warrants that each item of Equipment will conform in all material respects to the manufacturer's specification for a period of 12 months (apart from Software in which case for 90 days) from the date on which each item of Equipment is dispatched (the "Warranty Period") unless special conditions associated with certain Equipment apply.

4.3 All risks of loss or damage to QIoT Remote Monitoring shall pass to you on delivery. Property in the QIoT Remote Monitoring shall not pass to you until the purchase price has been paid in full. The solution shall remain the property of QIoT at all times.

4.4 Any QIoT Remote Monitoring delivered damaged must be notified to QIoT Ltd within 3 working days and returned to us within 6 working days of the order being delivered. We may, entirely at our discretion, repair or replace such damaged QIoT Remote Monitoring, substitute substantially similar goods or reimburse the price paid for the damaged QIoT Remote Monitoring.

4.5 The warranty set out in this clause shall not apply where the Equipment have been altered in any way or been subjected to misuse, including without limitation being dropped in water or any other liquid, or to unauthorised repair

5. Charges and Payment:

5.1 You have to pay for all charges for your QIoT Remote Monitoring and for using the Service as set out or referred to on the Order Form or in the Tariff you have chosen on the Order Form, including without limitation all Call Charges, Connection Charges, Monthly/Annual Rentals and QIoT Remote Monitoring Prices. You

acknowledge that you are responsible for paying all call Charges made using your QIoT Remote Monitoring and/or SIM Card whether or not such call has been made by your personally.

5.2 Unless expressly stated otherwise, all charges and prices for Services and QIoT Remote Monitoring supplied under this Agreement are exclusive of VAT, which shall be charged at the rate and in the manner prescribed by law from time to time.

5.3 We must receive payment from you for charges before service commences unless you are an organisation where 14 days invoice terms may be granted.. Payments must be made by BACS, Credit or debit card or direct debit. Any other payment method can only be made with prior written approval by us and may attract a surcharge of £5.

5.4 If we receive payment later than the timescales show in clause 5.3 above, we may charge interest on the amount outstanding. Interest will be charged at the rate of 2% above the base-lending rate of Yorkshire Bank from the date the amount becomes due to the date of full payment.

5.5 All sums due to us must be paid in full without set-off, counterclaim or deduction.

5.6 If applicable, we may set monthly credit limits for call charges where you pay in arrears. We may stop you using some or all of our Services if you go over the credit limit.

5.7 You must tell us within 1 months of your payment date if you have a query on any of your payments to QIoT. Any dispute in respect to an invoice must be submitted to us in writing within 1 months of the date of the invoice failing which it will be deemed agreed and accepted.

6. Intellectual Property

6.1 In the event that QIoT Ltd or its subcontractors supply software to you for use in conjunction with the Service, QIoT Ltd grants You, so far as QIoT Ltd is able, a nonexclusive, non-transferable licence for the use of such software for the duration of this Agreement. Except as permitted by law, the Customer is not permitted to copy, de-compile or modify the software, nor copy the manuals of documentation supplied with such software.

6.2 If requested by QIoT Ltd, the Customer shall sign any agreement containing reasonable terms which is reasonably required by the owner of the copyright in such software to protect the owner's interest in that software. No additional charges will be payable under such agreement.

7. Your Use of the Service:

7.1 You must not use your QIoT Remote Monitoring (or allow it to be used) for any illegal, fraudulent, or immoral purpose or to make offensive or nuisance calls. We may report any incidents to the police of any other relevant official organization.

7.2 You must not use you QIoT Remote Monitoring with any equipment, which has not been approved for use on the Network. If you are not sure, you should ask the person selling the equipment or you can call the following helpline number: 01415 010 450.

7.3 You agree to follow all reasonable instructions we provide you with regarding your use of the Service (for example, fair usage policy), and provide us with any information we reasonably ask for.

7.4 You must tell us immediately if your name, company name, address, bank account or credit card details change.

7.5 You agree not to use our service for anything other than the specified solution/s.

7.6 You agree that in respect of the service that QIoT Ltd is acting as a service provider and as such has no knowledge of, involvement with, or liability for the specific content of any messages sent to the Users SIM Cards, which do not originate for the Service Provider.

8. How You Can End or Terminate this Agreement:

8.1 You can end the agreement immediately if we have broken this agreement and cannot sort out the situation within 14 days of you telling us about the breach in writing.

8.2 You can end this agreement immediately if we do not give you Service for 30 consecutive days or more (by giving us written notice specifying the reason) unless you have broken this agreement or a matter covered in clause 13 or 18 occurs.

8.3 You can end this Agreement by giving us 30 days written notice to expire at the end of the initial Term or each anniversary thereof.

8.4 You can end this agreement by giving us 30 days written notice to expire before the end of the term

9. What You Have to Pay When You End this Agreement:

9.1 If you end this agreement for any reason, you will have to pay the charges you owe on your account and any unpaid invoices for QIoT Remote Monitoring.

9.2 If you end this agreement under clause 8.1 or 8.2 and you have paid the monthly charges in advance then you are not entitled to a refund or part refund of the Service.

9.3 In addition to the amounts payable under clause 9.1 above, if you end this agreement early under clause 8.4, you must pay:

9.3.1 The monthly line rentals for the part of the Term you have not used. The terms of this Agreement will continue to apply to paying off these charges; and

9.3.2 £25 per user for the cost of disconnecting your QIoT Remote Monitoring from the Network.

9.4 The prices of QIoT Remote Monitoring supplied under this Agreement are calculated by QIoT direct and may change without notice. Therefore, if you end this agreement under clause

9.5 prior to the expiry of the Initial Term for any QIoT Remote Monitoring supplied, you must either return any devices to us in good working order and condition or if you wish to keep them you must pay us the difference between what you had paid us for the QIoT Remote Monitoring and their full wholesale price. This may be up to £250 per device.

10. Right to Cancel for Consumer Purchases:

10.1 If your purchase is for personal usage (i.e. The Personal Details on the Order Form contained within the Service Agreement was completed rather than the Business Details, you can cancel your order for the Service and/or QIoT Remote Monitoring within the first 7 working days of receipt of the QIoT Remote Monitoring and/or Services.

10.2 On cancellation, you must return your QIoT Remote Monitoring device/s to us in the same condition as they were delivered to you (including the original packaging and any accessories that were included in the price), and we will refund you the purchase price you have paid.

10.3 On cancellation, you must also pay for any Charges and use of the Service you have made

11. How We Can End This Agreement:

11.1 We can end this agreement immediately if you become bankrupt, insolvent or go into liquidation or if you enter into a voluntary arrangement or have a receiver or/and administrator appointed over any or all of your assets. We do not have to give you notice in these circumstances.

11.2 We can also end this agreement in the following circumstances:

11.2.1 If you break this agreement and do not fully resolve the situation within 14 days of us telling you about the break. An example of a break of this agreement is not paying your invoices.

11.2.2 If the Network closes down for any reason.

11.2.3 If you give us false information

12. What You Have to Pay When We End this Agreement:

12.1 If we end this agreement because you break it, become bankrupt, or go into liquidation, or provide us with false information you will have to pay us all the charges set out in clauses 9.1, 9.2 and 9.4 above that you would have paid if you had ended this Agreement early under clause 8.4 and/or return to us any QIoT Remote Monitoring that are still subject to an Initial Term.

12.2 If we end this Agreement because the Network closes down, you will only have to pay the charges you already owe.

13. What to do if your QIoT Remote Monitoring's lost, stolen, or damaged:

13.1 You must inform us immediately if a device supplied to you by us is lost, stolen or damaged. You will remain liable for all Charges incurred until you do so. We will send you a replacement device as soon as reasonably practicable, but we reserve the right to charge you for doing so.

13.2 If you need us to replace a QIoT Remote Monitoring because it has been lost, stolen or damaged, we reserve the right to charge you the full price of any replacement.

14. Limits of Liability:

14.1 We are only liable to you as set out in this Agreement. We have no other duty or liability to you.

14.2 Nothing in this Agreement shall limit or exclude our liability for death or personal injury resulting from our negligence or that of our employees or for fraudulent misrepresentation or any other liability, which may not by applicable law be excluded or limited.

14.3 Except as set out in clause 14.1 above, our entire liability to you for something we or anyone who works for us does or does not do in connection with this Agreement and the equipment and services supplied by us is limited to £2,500 for one incident and to £5,000 for all incidents in a 12 month period.

14.4 We shall not be liable to you in any way for any loss of income, business or profits, loss of data or for any loss or damage that was not reasonably foreseeable at the time you entered this agreement.

14.5 We are not liable to you in respect of any products or services you order from other companies using your QIoT Remote Monitoring.

14.6 We will not be liable to you if we cannot carry out our duties or provide our services because of something beyond our reasonable control.

14.7 Where your QIoT Remote Monitoring allows access to the Internet, we shall not be liable to you for the content of any website or other material that you access via the Service.

14.8 Clause 7 will apply even after this Agreement has ended.

14.9 You accept this is not an emergency response service and in no way constitutes such a service, you also accept that the QIoT Remote Monitoring solution, software and all devices is a statistical analysis tool and only to be used as a guide in supporting your asthma to help you self-manage based on such statistical analysis.

14.9.1 You accept that all data extracted from the QIoT Remote Monitoring solution and all supporting devices is only to be used for statistical analysis as it may not be entirely accurate due to outside influences such as lack of coverage of cellular connectivity, software glitches and user error.

15. Refund Policy:

15.1 A refund will be granted within 30 days of purchase for:

15.1.1 Software supplied which is defective at the time of purchase and provided it has not been tampered with or altered in any way by you.

15.1.2 Software not delivered on the delivery date due solely to an error by QIoT Ltd.

15.2 We cannot offer refunds in the following instances:

15.2.1 Time purchased after a trial period has been used.

15.2.2 Over 14 days have elapsed from the date of purchase.

15.2.3 Software purchased for use on Networks not supported. Note: Where a refund is available to you a £5.00 administration fee will be charged if it is as a result of circumstances beyond Abzorb Solution's control.

16. Service Availability and Suspension:

16.1 We shall use all reasonable endeavours to provide and maintain the availability of the Service. However, we do not warrant that the Service shall be available without interruption or that it will be free from error. We may suspend the Service immediately if:

16.1.1 The Network fails or if it is being modified, maintained, or repaired, or if the Network is unavailable for any other reason.

16.1.2 You tell us about the loss or theft of your Device (but you must still pay the service charges under this agreement for any services contracted).

16.1.3 If we do not receive full payment for any of your invoices in time or you exceed any credit limits set under clause 5.6.

16.1.4 If we reasonably suspect or know your Device is being used fraudulently or illegally.

17. What You Must Pay if the Service is Suspended:

17.1 If the Service is suspended for reasons set out in clause 16.1 for more than 30 days in any month you will not have to pay line rental for that period.

17.2 If the Service is suspended for any of the reasons set out in clauses 16.1.2, 16.1.3 and 16.1.4, you will still have to pay the monthly line rental.

17.3 If we bar your access to the Service for non-payment of invoices, we shall charge you a fee of £35 per QIoT Remote Monitoring for reconnection.

18. Changes to this Agreement:

18.1 We can change the terms of this Agreement by giving you notice if the law or any regulations affecting the Service changes or VAT or any other tax is increased,

18.2 We can change our charges for the Service on 30 days written notice. However, if we increase our charges or introduce new charges because of something other than a change in the law or an increase in taxes, you can end this agreement on 30 days written notice. You will then only have to pay invoices for Services and QIoT Remote Monitoring that you incur up until the end of the notice period. During the notice period the old charges will still apply.

18.3 We shall notify you of any changes by mail, email, or text message to your Mobile Device

19. Transferring this Agreement:

This agreement is non transferrable by the end use but QIoT Ltd may sell the service and the clients within the agreements to another vendor/company without prior written notice after which the new vendor will write to the end user to notify them of any new terms to the contract.

20. Ownership of the Device:

20.1 We may change or reallocate your QIoT Remote Monitoring service where required to do so by any UK statutory or regulatory authority.

21. Coverage:

21.1 Your Device will only work in the areas covered by your mobile Network provider.

21.2 We cannot guarantee coverage in any area as we have no control over this but you can get coverage information from us. The Service may be affected by interference caused by the weather, high buildings, geographical feature, and tunnels

22. Use of Your Details:

22.1 For the purposes of fraud prevention, debt collection, credit management and emergency services provision, you agree that we may disclose information about you and your account with us to debt collection agencies, credit reference agencies, financial institutions, emergency service organizations and other Device companies. We may also pass you details to third parties in the event that we sell our business in order that you can continue to receive a QIoT Remote Monitoring Service.

22.2 Unless you indicate otherwise on the Order Form, we may also use you details to send you information and other services that we offer that we think you may be interested in.

23. No Third-Party Rights:

Under the terms of this Agreement a person who is not a party to this Agreement has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Agreement but this does not affect any right or remedy of a third party which exists or is available apart from by that Act.

24. Disputes and the Law:

24.1 Any concession or extra time we allow you under this Agreement applies only to the specific circumstances in which we give it. It does not affect our rights or remedies under this Agreement in any other way and will not constitute a waiver of our rights.

24.2 If any term or part of this Agreement is not legally effective, it shall not affect the enforceability of the remainder of the Agreement. The parties shall also agree that any ineffective or unenforceable term or part of this Agreement shall be substituted with a provision as similar in meaning to the original as is possible without rendering it unenforceable or ineffective.

24.3 You have the right to refer any disagreement regarding the service to an Arbitration Procedure. This was set up by the Chartered Institute of Arbitrators and the Network operators and we will provide details on request.

24.4 This Agreement shall be governed by the laws of Scottish Law.