InterAktive

Terms and Conditions

Contents

Acceptable Use Policy

1.0 Overview

InterAktive Ltd is committed to protecting the business, its customers and its employees from illegal or damaging actions by individuals, either knowingly or unknowingly.

The purpose of this policy is to outline the acceptable use of our computer equipment and computer applications, predominantly InterAktive. These rules are in place to protect the user and InterAktive Ltd from risks such as virus attacks, compromise of the network systems and services and legal issues.

Maintaining the robust security of InterAktive is a team effort involving the participation and support of all of us.

InterAktive Ltd has an established culture of honesty, openness, trust and integrity and it is not the intention of this policy to undermine any of those guiding principles and values of the business.

It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Scope

This policy applies to employees, contractors, consultants, temporaries, and other partners at or working for InterAktive Ltd, including all staff affiliated with third parties. This policy applies to all equipment that is owned or leased by InterAktive Ltd, and includes activities that may include 'own equipment' to access InterAktive.

3.0 Policy

3.1 General Use and Ownership

1. While InterAktive Ltd wishes to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of InterAktive. Because of the need to protect InterAktive's network, management cannot guarantee the confidentiality of information stored on any network device belonging to InterAktive Ltd

2. Employees are responsible for exercising good judgement regarding the reasonableness of personal use. Refer to ProAktive HR Policies for further

information and if there is any uncertainty, employees should consult their line manager.

3. For security and network maintenance purposes, authorised individuals within InterAktive or our IT Partners, currently Quadris, may monitor equipment, systems and network traffic at any time as per ProAktive's monitoring policy.

4. InterAktive Ltd reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

3.2 Security and Proprietary Information

1. Confidential information is all information provided by clients and which is stored on InterAktive. Employees should take all necessary steps to prevent unauthorised access to this information.

2. Users should keep passwords secure and must not share accounts. Authorised users are responsible for the security of their passwords and accounts. InterAktive administrator level passwords should be changed monthly and any other user level passwords should be changed every 3 months

3. All PCs, laptops and workstations should be secured with a password-protected screensaver and users should log-off when they leave their workstation unattended.

4. All equipment used by the employee that are connected to the InterAktive network, whether owned by the employee or InterAktive, shall be continually executing approved virus-scanning software with a current virus database as per Quadris instruction.

5. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which could contain viruses, e-mail bombs, or Trojan horse code.

6. Employees must not request or save any passwords on behalf of clients, and if manual resetting is necessary to give a client access they must be advised to reset their password to something strong but memorable.

3.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities. Please note that InterAktive administrators have a high level of permission which may grant them access to areas that they do not require to access in the normal course of their role. InterAktive administrators should not access any information to which they are privileged unless requested to do so by a senior member of staff or in order to execute the normal course of their role.

Under no circumstances is an employee of InterAktive Ltd authorised to engage in any activity that is illegal while utilising InterAktive owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

3.4 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violation of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar in laws or regulations, including, but not limited to, the installation or distribution of “pirated” or other software products that are not appropriately licensed for use by InterAktive

2. Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which InterAktive Ltd or the end user does not have an active license is strictly prohibited.

3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

6. Using an InterAktive Ltd computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

7. Make fraudulent offers of products, items, or services originating from any InterAktive Ltd account.

8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorised to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

10. Port scanning or security scanning is expressly prohibited unless prior notification to InterAktive is made.

11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job\duty.

12. Circumventing user authentication or security of any host, network or account.

13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet

15. Providing Information about, or lists of, InterAktive Ltd employees to parties outside InterAktive Ltd.

InterAktive Data Backup / Business Continuity Policy

Data stored within InterAktive is backed up according to the following policy objectives:

1. Hourly backups take place from 8am to 6pm each day and are held for 7 days. These may be recovered within 7 days of the backup taking place. Following this a weekly back up is held for 4 weeks which subsequently turns to a monthly backup. Monthly back ups are held for 36 months.

Backup Policy	Retention
Hourly backups taken 8am to 6pm each day	Held for 7 days
Hourly backups reduced to daily backups after 7 days	The daily backup held for a further 7 days
Daily backups turned into weekly backups after a further 7 days	Weekly backups are held for 4 weeks
Weekly turned into monthly	Monthly backups are held for 36 months

The above data policies provide the following protection to your data:

In the event of a system failure, no more than one hour of data should be lost assuming that the failure takes place between 7am and 7pm. Outside of these hours data loss will be from the time of failure and the previous backup at 6pm.

In the event of lost or corrupt data needing to be recovered the following can be achieved:

- Within 7 days of the loss or corruption we can recover back to the nearest hour.
- Between 8 days and 14 days we can recover data if it existed in the system at the end of a day.
- From 15 days to 4 weeks we can recover data if it existed in the system at the end of a week. I.e. if a data was created on a Monday and deleted a day after (on a Tuesday), after 15 days we could not recover it because it wasn't on the week end backup.
- For data older than 4 weeks it can be recovered if it was present on a month end backup for up to 36 months.

2. Backed up data sets are encrypted and synchronised to another UK based data centre where it can be recovered from, thus reducing reliance on a single data centre.

3. The primary data centre is ISO27001 accredited and is very secure and has high levels of business continuity protection. In the event of a loss of the entire data centre, the complete system can be recovered to the standby data centre within 4 hours. In this event the maximum loss of data would be 1 hour assuming the disaster

occurred between 7am and 7pm. Outside of these hours it would be the time from the disaster event to the previous backup at 6pm.

The data centre housing the InterAktive system has the following resources which deliver high levels of business continuity protection:

1. Smoke detection system
2. Overhead and under floor fire suppressant equipment
3. Un-interruptible power supply to the entire data centre and to each server hosting InterAktive
4. Climate control
5. Resilient connection to the internet

Excess Storage Fees

The customer shall have an allowance of 5GB of storage space. Data storage over this limit shall be charged at the fees of £1.50 per annum per GB thereafter.

InterAktive Privacy Policy

InterAktive is committed to protecting its customer data from unauthorised access. Authorised access will include:

1. Employees and representatives of clients who have been granted permission by the customer to the system

2. Employees of InterAktive required to access client information required to carry out the service

3. Employees of appointed contractors of InterAktive required to technically administer the system

4. Service Partners. This only applies where a site has been built for a Service partner who allows for their clients to access the system and it is a requirement that the Service Partner has access to their client's information.

Unauthorised access is any other person or party not included in the above definition. Access by unauthorised persons or parties is controlled by the following security controls which are typical of many web based software services:

1. SSL encryption of data transmitted between the user's browser and InterAktive's servers.

2. A firewall to restrict access to the network except through authorised ports.

3. Use of self-managed login credentials that use complex passwords which reduces the risk of the password being compromised by automated malicious systems and individuals.

4. Use of Microsoft's proprietary security architecture built into the software that runs Interaktive.co.uk.

5. Access is granted to internal InterAktive employees on a need to know basis.

The InterAktive system is hosted on infrastructure in a specialist data centre which has the following security features:

1. 24 hour security

2. CCTV both internal and external

3. Access to authorised personnel using a positive identification procedure

4. 7ft high security fence around the perimeter of the building, secure access to the building controlled by permanent data centre staff and electronic padlocks to each server cabinet

InterAktive Security Policy

InterAktive takes security extremely seriously and this document explains the security measures we use to protect your data when using our InterAktive Portal.

Data Centre Facility Security

Our InterAktive portal is hosted in a purpose built data centre facility in the North East of England which has been awarded the British Standard 7799 and ISO 27001 security standards. BS7799 is a certification for dedication to making customers systems and information resilient and secure. ISO27001 is a globally recognized certification for data security. The facility is unmarked and ideally paced 60m above river levels to reduce the risk of flooding. The rest of this section provides further detail of the data centre capability.

Security

The data floor, all access routes and areas outside the building are monitored by a CCTV system with intruder detection, which comply with all NACOSS standards. 20 CCTV cameras in total, 12 external which store all data captured for 2 weeks and 8 internally which store data for 2 years. The data centre is a non-descript building surrounded by a 7ft high perimeter fence. Entry to the data floor can only be gained at the discretion of a data centre engineer and the data racks housing our servers are secured by electronic key pad locks to ensure that only authorised personnel are able to gain access. An

audit trail of personal movements and area access is retained for security and reporting purposes.

Fire Protection System

The Facility is protected by the latest overhead and under floor FM200 fire suppressant technology. The data centre is monitored by a series of highly sensitive smoke detectors which will emit a safe, clean gaseous combination of argon, carbon and nitrogen to extinguish the fire without damaging electronic equipment.

Bandwidth

Bandwidth in excess of 1GBps is provided from multiple providers with diverse feeds, including Global Crossing, British Telecom, Cable and Wireless and Onyx Group.

Un-interruptible Power Supply (UPS)

The UPS system ensures that the facility remains fully operational 100% of the time. The data centre has dual diversely routed high voltage (11kV) power feeds delivering power to a dedicated sub-station and has never experienced a mains failure. However, in the unlikely event of the data centre losing power the system will maintain supply to the data floor until the 800KVA back-up generator containing 11,000 litres of diesel takes over. There is sufficient diesel held on-site for the generator to run on a full load for over 48 hours, and they have a 24 x 7 refuelling contract in place, in case of a prolonged power cut.




Climate Control

The data floor environment is controlled by N+1 air-conditioning units to ensure it is maintained at 22 degrees Celsius – the optimum temperature for servers and electronic equipment. There is a cold aisle/hot aisle scenario in place, cold air circulates under the floor whilst the servers bring in the cold air through the front and send hot air out at the back. The data centre utilises 7 air conditioning units each with 40KW of cooling with 280KW current, there is scope for another 120KW. This means The air-conditioning system will support the data centre at maximum capacity with redundancy to protect against unit failures.

Disaster Recovery Solution

Ensuring our client data is protected from potential threats is a priority for us. Data is backed up every night to tape and stored in a fire proof, locked vault in the data centre.

Authorised Access

The InterAktive portal is administered by a small group of dedicated InterAktive / ProAktive personnel. This team is responsible for granting your users access to your data and ensuring only they have access.

Protection Against Unauthorised Access

As well as the physical security mentioned previously, access to the InterAktive network hosting the portal is protected by a resilient Cisco ASA firewall and intrusion detection. The system is monitored 24 x 7 by our dedicated I.T. support partner, Quadris. The monitoring includes:

- Monitoring of firewall logs
- Automated alerting of all critical system events
- Monitoring data backup and replication jobs
- Monitoring anti-virus scan logs

Data transmission between our clients PCs and servers is encrypted via SSL using a globally recognized security certificate provider. This is the same type of security used by banks.

We also enforce the use of strong passwords to protect against easily cracked weak passwords.

InterAktive Support Services Policy

The following InterAktive Support Agreement and Service Level Agreement combine to form the InterAktive Support Services Policy and apply to customers who have in place an Agreement with InterAktive and for which payment has been received.

InterAktive Support Agreement

1. **Introduction**

   InterAktive provides a support service for the named users of the InterAktive Portal Service, the details of which are set out in this Support agreement. The Support Agreement for the InterAktive Portal is made by InterAktive Ltd in connection with, and is part of your licensing agreement (the "Agreement"). This support agreement applies to the InterAktive Portal available at https://interaktive.co.uk.

2. **Contact Details**

   Our customer support team can be contacted via telephone on 01302 346825 or via email at info@interaktive.co.uk. The support service is available for any user of the Service, as defined in the Agreement.

3. **Hours of Operations**

   The support service shall be available during our normal business hours.

4. **Response and Resolution**

   We have a dedicated team of support staff who will respond to each support request within 3 hours of receiving the initial call or email. We aim to resolve all issues within 24 hours of receiving the support request. This is offered as a target and not a formal service level.

5. **Customer Obligations**

   The Customer acknowledges that issues experienced with the Service may be down to factors outside of the control of InterAktive. Where necessary, the Customer will make available employees or relevant 3rd parties that have knowledge of the Customer's computer network in order to help diagnose the issue.

   The Customer may be asked to allow InterAktive, or its authorised agent to connect to the Customer's network in order to assist in resolving a support request. Where

this is required the Customer will be notified and asked to permit the remote connection to take place. The Customer agrees to grant such permission as part of this Support Agreement.

6. **Definitions**

   a. Normal Business Hours: 9am to 5pm, Monday to Friday, excluding public holidays.

   b. Support Request: a telephone call or email requesting support in relation to the use of the InterAktive Portal.

Service Level Agreement

1. Introduction

This Service Level Agreement for the InterAktive Portal (this "SLA") is made by [InterAktive Ltd] in connection with, and is a part of, your licensing agreement (the "Agreement"). This SLA applies to the provision of the InterAktive Portal available at https://interaktive.co.uk.

We provide financial backing to our commitment to achieve and maintain the Service Levels for our Services. If we do not achieve and maintain the Service Levels for our Service as described in this SLA, then you may be eligible for a credit towards a portion of your monthly service fees. We will not modify the terms of your SLA during the initial term of your subscription; however, if you renew your subscription, then the version of this SLA that is current at the time of renewal will apply for your renewal term.

2. Definitions

"Applicable Monthly Service Fees" means the total fees actually paid by you for the Service that are applied to the month in which a Service Credit is owed.

"Downtime" means a period during which the InterAktive portal is unavailable, excluding (i) Scheduled Downtime; and (ii) unavailability of a Service due to limitations described in Section 5(a) below. Downtime is measured in the units set forth in Section 3.

"Incident" means (i) any single event, or (ii) any set of events, that result in Downtime.

"Scheduled Downtime" means periods of Downtime related to network, hardware, or Service maintenance or upgrades. We will publish notice or notify you at least two (2) days prior to the commencement of such Downtime.

"Service" or "Services" refers to the InterAktive Portal available at https://interaktive.co.uk indicated at the beginning of this SLA and purchased by you pursuant to the Agreement.

"Service Credit" is the percentage of the Applicable Monthly Service Fees credited to you following our claim approval.

"Service Level" means the performance metric(s) set forth in this SLA that we agree to meet in the delivery of the Services, e.g., monthly availability.

"User Minutes" means the total number of minutes in a month, less all Scheduled Downtime, multiplied by the total number of users.

3. Service Level Commitment

(a) The "Monthly Uptime Percentage" for a Service is calculated by the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}}$$

where Downtime is measured as the total number of minutes during the month when the aspects of the Service are unavailable.

(b) If the Monthly Uptime Percentage falls below 98.5% for any given month, you may be eligible for a Service Credit.

4. Service Credit Claim

If we fail to meet the minimum Monthly Uptime Percentage described above for a Service, you may submit a claim for a Service Credit.

You must submit a claim to our customer support team by the end of the calendar month following the month in which the Incident occurred. For example, if the Incident occurred on February 15th, we must receive the claim and all required information by March 31st.

We will evaluate all information reasonably available to us and make a good faith judgment on whether a Service Credit is owed. We will use commercially reasonable efforts to process claims during the subsequent month and within forty five (45) days of receipt. You must be in compliance with the Agreement in order to be eligible for a Service Credit. If we determine that a Service Credit is owed to you, we will apply the Service Credit to your Applicable Monthly Service Fees.

5. Limitations

(a) This SLA and any applicable Service Levels do not apply to any performance or availability issues:

1. Due to factors outside our control (for example, natural disaster, war, acts of terrorism, riots, or government action);
2. That result from your or third party services, hardware, or software;
3. Caused by your use of a Service after we advised you to modify your use of a Service, if you did not modify your use as advised;
4. During pre-release, beta and trial Services (as determined by us);
5. That result from your unauthorised action or lack of action when required; or
6. That result from your failure to adhere to any required configurations, use supported platforms, and follow any policies for acceptable use.
7. For licenses reserved, but not paid for, at the time of the Incident.

(b) Service Credits are your sole and exclusive remedy for any performance or availability issues for any Service under the Agreement and this SLA. You may not unilaterally offset your Applicable Monthly Service Fees for any performance or availability issues.