Resman Limited

and

[Party 2]

IT Security Policy

POLICY NUMBER	**2020-07**
RATIFYING ENTITY	[**CLIENT NAME**]

Policy Statement:

[**CLIENT NAME**] recognises the importance of a structured, coherent and secure information system and associated systems to manipulate, communicate and store information to enable the organisation to conduct its business in a structured and secure manner and in accordance with best practice.

22 Rose Lane
Liverpool
L18 5ED
UK

Table of Contents

1. Rationale

1.1 The IT Security policy has been put in place for the following reasons:

(a) [**CLIENT NAME**] recognises the importance of information and information systems for the transfer, manipulation and storage of information to ensure operations and business continuity.

(b) The security of staff, company and client information is paramount to [**CLIENT NAME**].

1.2 [**CLIENT NAME**] wishes to ensure:

(a) Availability - to ensure that information assets are available as and when required in line with our business objectives.

(b) Integrity - to protect information assets from unauthorised or accidental modification and so maintain effective operations.

(c) Confidentiality - to protect information assets from unauthorised access and disclosure.

1.3 Through this policy, government laws and legislation, [**CLIENT NAME**] will identify and adopt a structured security procedure for our information systems.

1.4 In addition, all staff are bound by the confidentiality and security policies set out in this document together with their contractual obligations, and by the common law duty to maintain confidentiality concerning the data and information they use as part of their everyday work within our organisation.

2. Scope

2.1 All information that is created, processed, stored, transmitted or received during the course of our business activity is an asset of the organisation and as such is governed by this policy.

2.2 This policy applies to all employees or other persons working for [**CLIENT NAME**] or whilst engaged on or involved in any [**CLIENT NAME**] business activity and to any other users whilst using [**CLIENT NAME**] computers.

2.3 The policy applies to all [**CLIENT NAME**] sites and places of work (including home) that are used to conduct our business.

2.4 This policy must be adhered to at all times. Failure to comply with this policy may lead to our disciplinary policy being invoked.

3. Principles

3.1 The term 'Information' can be defined as "a collection of facts or data" and for the purpose of this policy includes information stored on computers and transmitted across networks, i.e. information that is retrieved, accessed, transmitted to, or received from other organisations using networks (Local or Wide) including internet and remote access and any other communications, media, and stored on disk, tape or any other electronic or optical media.

3.2 Also included are verbal communications and any other methods used to convey knowledge and ideas relating to [**CLIENT NAME**] or its business.

3.3 Appropriate protection is required for all forms of information to ensure business continuity and to avoid breaches of the law and statutory, regulatory or contractual obligations.

4. Laws Legislations and Guidelines

4.1 Due to the nature of our business, [**CLIENT NAME**] must comply with but is not limited to, the following laws, legislations and guidelines:

(a) Data Protection Act 2018 (the "**2018 Act**") and the EU General Data Protection Regulation ("**GDPR**")

(b) The Computer Misuse Act 1990.

(c) Electronic Communications Act 2000.

5. Information Confidentiality

5.1 Keep all confidential information secure, use it only for the purposes intended and do not disclose to any unauthorised third party.

5.2 If a document is highly confidential or sensitive in nature, you must store it in a private directory or an equivalent password protected directory. It should be noted that documents in common directories can be accessed by other employees.

5.3 All data stored within [**CLIENT NAME**] is subject to the Data Protection Act 2018 (the "**2018 Act**") and the EU General Data Protection Regulation ("**GDPR**"). Any person copying data from a source and storing it on a 'Home' network drive will need to adhere to the Act's stated principles with that data, in particular:

(a) Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.

(b) Personal data shall be accurate and, where necessary, kept up to date.

(c) Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

(d) Copies of confidential information should only be printed out as necessary, retrieved from the printer immediately, and stored or destroyed in an appropriate manner.

(e) Staff who roam between locations need to be aware at all times of what printer settings they have set. It is unacceptable to print documentation for one location to another location and vice versa.

(f) Do not leave documents containing client information open on any monitor. Always log out or lock your computer when leaving your desk.

(g) Where possible position your monitor so as to not let other members of staff oversee what is on your screen.

5.4 Any documents containing any client identifiable information must not be saved to the workstation or device's local storage (e.g. "C" drive), USB devices, CD/DVD/Blu-Ray, Memory Card or any other external storage devices even those that are encrypted), unless via an approved methodology.

6. Policy

This security policy covers all [**CLIENT NAME**] owned systems and information communicated and managed by these systems.

6.1 Email

[**CLIENT NAME**] employs the use of email to facilitate business objectives. Microsoft Outlook via MS Exchange is used for day to day communications of non-secure information and is set up as part of the account request process. Sensitive mail can be manually encrypted to any external recipient. Emails and attachments or anything that is considered sensitive or would bring [**CLIENT NAME**] into disrepute is prohibited. We reserve the right to invoke the disciplinary policy for any failure to comply with this policy.

6.2 Personal Use

(a) Although personal use of email facilities is discouraged, limited personal use will be permitted provided that the content of messages are appropriate, i.e. is not likely to cause offence and is not used for personal, business or financial gain and that a Director has agreed to its use.

(b) Employees should regard this facility as a privilege that should be exercised in their own time without detriment to their job and not abused.

(c) Inappropriate use may result in disciplinary action and/or removal of facilities. However, staff should be aware that both private and business use of email will be subject to monitoring.

6.3 Confidentiality

(a) Confidentiality can be compromised when using email systems and vigilance is required at all times. If in the unlikely event an email is sent to the wrong person, then the recipient person could read the email. Staff are actively encouraged to check recipient email addresses before sending emails so as to minimise the chances of this happening. In the unlikely event that this situation were to occur and as a precaution, all outgoing emails carry a disclaimer wording.

(b) When communicating client related data the minimum amount of client identifiable information necessary must be used. Staff should seek advice from a Partner regarding sending confidential information via email. The principles of the Data Protection Act 2018 (the "**2018 Act**") and the EU General Data Protection Regulation ("**GDPR**") should be adhered to at all times.

6.4 Housekeeping

(a) The amount of email in personal inboxes should be kept to a minimum. Non-essential work related emails should be deleted after reading, response, or action. Saved emails must be reviewed on a regular basis and deleted when no longer required.

(b) It is good practice to move emails that need to be saved to a personal folder. The same housekeeping rules apply to Sent Items. Care must be taken when sending file attachments as these are typically large and may cause network congestion. File attachments must only be sent when necessary and must be deleted as soon as is practicable. Users are responsible for their own housekeeping. Staff should refrain from sending emails with inserted graphics, multimedia or large attachments unless absolutely necessary, as these emails tend to take up a lot of space on the system.

6.5 Use of Email

(a) [**CLIENT NAME**] uses technologies and policies to control who has access to our network and these policies also control who has access to the email systems and at all times the following procedures are to be adhered to:

(i) expressly agree with any recipient that the use of email is an acceptable form of communication bearing in mind that if the material is confidential, privileged, or sensitive, that email is normally un-encrypted and is not secure unless specifically manually encrypted;

(ii) some intended recipients may have rigorous email gateway protocols (or firewalls) which can automatically screen all incoming email for content and source. If this is the case, consider whether this means of communication is appropriate; and

(iii) all emails are checked for viruses and content.

6.6 Terms of Use

(a) The main purpose in providing IT facilities for email is to support the approved business activities of [**CLIENT NAME**]. IT facilities provided for email should not be abused. An absolute definition of abuse is difficult to achieve but certainly includes and is not necessarily limited to:

(i) creation or transmission of material that could bring [**CLIENT NAME**] into disrepute;

(ii) creation or transmission of material that is illegal;

(iii) the transmission of unsolicited commercial or advertising material, chain letters, press releases or other junk mail of any kind;

(iv) the unauthorised transmission to a third party of confidential material concerning the activities of [**CLIENT NAME**];

(v) the transmission of material such that this infringes the copyright of another person, including intellectual property rights;

(vi) activities that unreasonably waste staff effort or networked resources, or activities that unreasonably serve to deny service to other users;

(vii) activities that corrupt or destroy other users' data or disrupt the work of other users;

(viii) unreasonable or excessive personal use.;

(ix) creation or transmission of any offensive, obscene or indecent images, data or other material.;

(x) creation or transmission of material that is designed or likely to cause annoyance, inconvenience or anxiety;

(xi) creation or transmission of material that is abusive or threatening to others, serves to harass or bully others, discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status and disability, political or religious beliefs;

(xii) creation or transmission of defamatory material or material that includes claims of a deceptive nature;

(xiii) activities that violate the privacy of others or unfairly criticise or misrepresent others, this includes copying distribution to other individuals;

(xiv) creation or transmission of anonymous messages or deliberately forging messages or email header information, (i.e. without clear identification of the sender);

(xv) the deliberate unauthorised access to services and facilities; and

(xvi) the unauthorised provision of access to [**CLIENT NAME**] services and facilities by third parties.

6.7 Spam and Junk Email

(a) Spam can be defined as "the mass electronic distribution of unsolicited email to individual email accounts". Junk mail is usually a result of spamming however in reality, spam and junk mail are regarded as interlinked problems.

(b) [**CLIENT NAME**] maintains an email content management system (gateway) which filters junk email, any mail reaching the email gateways which has been marked as junk mail will be quarantined on the gateway and will not be delivered.

(c) [**CLIENT NAME**] is constantly striving to improve its junk mail detection mechanisms but unfortunately no system is 100% and occasionally junk email will evade the detection process and be delivered. Conversely some mail may be tagged as junk mail but is legitimate.

6.8 Virus Checking

Computer viruses, Trojan horses and worms are collectively known as malware. The most common method for distributing malware is via email. All email communications passing through [**CLIENT NAME**] email servers is checked for malware. Checking strategies include refusing messages containing executable attachments, scanning messages for known malware or a combination of both techniques.

6.9 Content Filtering

(a) Email is filtered at the message gateway for both inbound and outbound mail, and content filtering is in use to stop the exchange of any viruses, chain letters, spam etc.

(b) [**CLIENT NAME**] content filtering system is configured to reply to internal users informing them that their message has been blocked, detailing the reason for the block and advising on the actions required to have the message released.

7. Internet

7.1 [**CLIENT NAME**] employs the use of the internet as a communications medium to facilitate its business function. Access to the internet is controlled through network security.

7.2 Any person or persons accessing the internet via the [**CLIENT NAME**] network will be considered to have read, understood and accepted the IT Security policy.

7.3 Any client accessing the internet via [**CLIENT NAME**] network will have to comply with this policy.

7.4 The purpose of this document is to define the environment under which full or partial access to the internet may be granted from a workstation or device attached to our local network, and:

(a) To clarify our policy regarding staff use of the internet.

(b) To mitigate our exposure to potential liability.

(c) To minimise the risk of internet borne security threats through the promotion of staff awareness and good practice.

(d) To encourage the most effective and positive use of the internet as an information resource.

7.5 **Directors** are responsible for ensuring that users are aware of and conform to the practices laid out in this document.

7.6 The internet is a source of information and knowledge of infinite range but offers no guarantee of accuracy, reliability and authenticity.

7.7 The membership of special interest groups is not private and, the fact that a member belonged to [**CLIENT NAME**] would be easily apparent and could be used to generate adverse publicity.

7.8 Therefore, the use of [**CLIENT NAME**] email accounts must not be used for registering with internet sites for any personal business use including but not limited to eBay, Tesco, or other home shopping and holiday sites. We reserve the right to investigate any usage that may bring [**CLIENT NAME**] into disrepute.

7.9 It is recognised that social media is becoming an important channel for effective communication and as such viewing access is permitted during break and rest periods via agreement with a Director. Please ensure the Social Networking Security Standard is read and understood as part of this policy

7.10 Internet Use

(a) When entering an internet site, always read and comply with the terms and conditions governing it's use:

(i) do not download any images, text or material that is copyright protected (see Copyright, Designs & Patents Act 1988);

(ii) do not download any images, text or material that are obscene or likely to cause offence;

(iii) you must not download or install any software. Should you require to download or install any software, first seek permission from the Resman Helpdesk. Resman will check that the source is safe, and will keep a record of the licences for all software used including whether the software was free or paid for;

(iv) if you are involved in creating, amending or deleting web pages or content on our web site, such work should be consistent with your responsibilities and be in our best interests; and

(v) always ensure that the proper vetting procedures have been complied with and the information is accurate and up to date.

7.11 Personal Use

(a) [**CLIENT NAME**] has made arrangements for the internet to be used for the purposes of our business. The facility can be used for employees personal use at the discretion of the Directors and during a time agreed. The internet may also be used for educational purposes if this is identified as a necessary requirement for the development of a particular member of staff.

(b) Any abuse of this concession or failure to adhere to the terms under which such access is granted will be treated as a disciplinary offence. Please ensure that your personal use of the internet:

(i) does not interfere with the performance of your duties;

(ii) does not take priority over your work responsibilities;

(iii) does not incur unwarranted expense;

(iv) does not have a negative impact on [**CLIENT NAME**] in any way and is lawful and complies with this policy;

(v) is conducted during official breaks and outside working hours; and

(vi) is not used for personal business or financial gain.

(c) Any user found to be using the internet connection for conducting personal business activities will be subject to disciplinary action under our disciplinary process.

7.12 Internet Security

(a) The Internet is not a secure transport medium for information. Under no circumstances must client identifiable information be sent via the internet unless advice has been requested and permission given from Resman or a Director.

(b) Any attempt to gain unauthorised access to the internet will be treated as a disciplinary offence (see also The Computer Misuse Act) and will be dealt with under our disciplinarily procedures.

(c) The internet must never be accessed via any separate device (laptop type or mobile internet enabled device). The internet must only be accessed via the [**CLIENT NAME**] network and only via a [**CLIENT NAME**] owned/approved computer or device.

(d) All staff are responsible for the security of the workstation they access the internet from. After using the workstation staff must logout. If a breach of security is identified, the user's account that the offence occurred under will be investigated.

7.13 Monitoring

(a) All internet traffic is monitored and controlled 24 hours a day for network bandwidth, security purposes and content control. The systems used to monitor internet traffic are used to generate usage reports. These reports contain the following information:

(i) user name;

(ii) sites accessed;

(iii) time spent accessing the internet and individual sites; and

(iv) amount of information accessed.

(b) These access reports will be reviewed on regular bases for audit purposes.

7.14 Reporting

(a) If a member of staff feels that they have accidentally accessed an inappropriate internet site they should report this matter to a Director and the Resman Helpdesk as soon as possible.

(b) All staff have a responsibility to report any security incidents or suspected security incidents or any security vulnerabilities to systems or information to a Director.

7.15 Internet Content Filtering

(a) All internet traffic is checked for content via an internet content management system.

(b) The content management system checks for illegal or immoral sites, all access to these sites will be blocked, other sites which are blocked will include but are not limited to:

(i) gambling sites;

(ii) adult content;

(iii) games sites;

(iv) crime/terrorism; and

(v) music downloads.

(c) The system is updated by Resman therefore [**CLIENT NAME**] cannot be held accountable if any clients access internet sites of an unsavoury or dubious nature. If any member of staff feels they have access to any of the above mentioned sites they must report this to the Resman Helpdesk immediately.

8. Remote Working and Mobile Devices

Current models of working are such that staff may need to access [**CLIENT NAME**] information from a location that is not their normal work base. We provide a variety of mobile devices and allow the use of mobile storage where necessary. Please ensure the Remote Working and Mobile Devices Security standard is read and understood as part of this policy.

8.1 Site Security

(a) It is the responsibility of all staff to make their area of work as secure as is reasonably possible.

(b) Where possible, all IT server units and communications rooms must be locked at all times. This is for security and health and safety due to fire prevention systems in place.

8.2 Desktop Computer Security

(a) Desktop security is of paramount importance and as such Resman controls the following through network security:

(i) network account Password protection - network account password change will be requested every 90 days;

(ii) screen saver password protection - password protected screen savers will be activated if the computer is idle for 10 minutes; and

(iii) virus protection - the virus protection systems employed will automatically update while the computer is attached to our network and actively check all open files.

(b) Under no circumstances must staff copy any personal or multimedia files i.e. MP3, CDA, WMA, GIF, BMP or JPEG files which are not those of [**CLIENT NAME**] or related to any local or network drive. If any such files are found on staff accounts or shared drives, this will be classed as computer misuse and subject to our disciplinary process.

(c) Staff must remain vigilant at all times when working on client information.

(d) Do not use the system in any way, which may damage, overload or affect the performance of the system or the internal or external network.

(e) Use of non-[**CLIENT NAME**] IT equipment on our premises without authorisation from Resman Helpdesk will be classed as computer misuse and dealt with under our disciplinary procedures.

(f) It is the users' responsibility to make their area of work as secure as possible. We will put in place physical security measures to ensure the security of our assets as is reasonably possible.

(g) We have an asset management system in place to record all [**CLIENT NAME**] IT assets to enable us to maintain an accurate record of IT assets and to enable the availability of our systems.

8.3 Virus Protection

(a) [**CLIENT NAME**] recognises the potential threat to our information assets through malicious programmes and as such has put in place a system to check and remove viruses from our network. Each workstation that resides on our network will have the virus protection system installed and will be automatically updated whenever a new virus is discovered.

(b) We will try to protect our assets against the threat of viruses to our best endeavours and recognise the dangers that a virus could do if not detected and removed. It is also the responsibility of all staff to be vigilant and take steps to protect themselves against computer viruses.

(c) Staff must never attach or insert any external storage media into any [**CLIENT NAME**] computers without express permission from a Director and Resman and having it virus checked.

8.4 Network Security

(a) We recognise the need for a secure and reliable system to transfer information. To facilitate the transference of information we utilise a switched based network system.

(b) All [**CLIENT NAME**] network switches comply with but are not limited to the following standards:

(i) all switches are password protected;

(ii) only members of Resman have access to the switch passwords;

(iii) all switch passwords are changed if a member of Resman staff who has had access to the switch passwords subsequently leaves;

(iv) all switches must be located in a secure location; and

(v) all external network traffic containing client information is encrypted.

8.5 New Systems

(a) To aid business continuity we will from time to time implement new systems or update old systems.

(b) Any new IT based systems installed on the [**CLIENT NAME**] network or stand-alone systems must be implemented as part of a recognised and structured IT project. Any IT based systems must be in collaboration with Resman. This will ensure that the correct procedures are maintained for the integration of new systems regarding the location, protection and backup of any information produced or stored on or by the new systems.

(c) The following are some key issues used in project planning surrounding the integration of new IT systems:

(i) **Conformity**

To keep systems at the same or equivalent levels of standardisation.

(ii) **Continuity**

To ensure all new IT systems are available where and when they are needed and that all processed, and system dependent information is backed up in case of system failure.

(iii) **Security**

To ensure that any new systems are located in a secure location and under the correct environmental conditions (i.e. air conditioned and with the correct fire suppressant systems in use). To ensure that all data produced or processed by the new system is stored in a secure location. To ensure that the correct access levels to the new system are set up and password protection is used with an audit trail of system access.

(iv) **Support**

To ensure that staff are trained on any new systems to allow an acceptable level of support.

(d) It is therefore vital to [**CLIENT NAME**] that Resman are involved with any new system from the planning and procurement to the implementation and support of any new IT based systems and to ensure that any new applications comply to policies and guidelines.

8.6 System Access Levels

(a) [**CLIENT NAME**] employs different systems to facilitate our business function. Most systems have different access levels which allow users access to different levels of client information or access at an administration level. We reserve the right to add, remove or change access to applications or systems to facilitate our business functions.

(b) Access levels to our systems will be maintained by Resman using a secure and structured approach. This allows for a clear and concise audit trail of all access requests.

(c) Access to systems outside the administrational control of Resman will be controlled by the companies, department or persons supporting these systems. Request for access or change of access must be via the companies, department or persons supporting these systems and be undertaken in conjunction with Resman in a controlled environment.

9. Disposal of IT equipment and Media

We will dispose of our assets and IT equipment in a controlled and secure manner in accordance with best practice guidelines.

10. Password Management

10.1 Passwords are confidential information and must be treated as such. A password is only as secure as the person who knows it and as such the following standards must be adhered to:

(a) Keep your system passwords safe.

(b) Do not disclose them to anyone.

(c) You will be forced to change your passwords from time to time for security purposes and in line with guidelines.

(d) Network passwords must be a minimum of 8 characters and at least one character should be nonalphabetic.

(e) Should be easy to remember but difficult to guess.

(f) Should not relate to information that is known to other members of staff.

(g) Each user is responsible for maintaining the security of their individual log in and password.

(h) Staff must not share their user name or password with anyone.

(i) Must not be written down unless kept in a sealed envelope and locked in a drawer or otherwise securely held by a Director.

10.2 Each user is responsible for maintaining the security of their individual log in and password. If a breach of security is recorded under your log in the burden of proof will be on you to show that you are not responsible for the breach.

10.3 All passwords should be changed at regular intervals when requested by the system. This should be no less than 90 days. If a password is forgotten please call the Resman Helpdesk to obtain a new password.

10.4 This policy covers passwords that are used for access to systems that have been installed and are maintained by Resman. Passwords used for other computer-based systems will be the responsibility of the companies, departments or persons supporting these systems.

11. Network Account Management

All IT network accounts will be created and maintained by Resman. Network audits will be conducted to check account assignments and user rights are being maintained.

11.1 Account Creation

All new network accounts must be requested by a Director using the starter request form.

11.2 Account Deletion

If a member of staff leaves, a leaver form will be completed and sent to the Resman Helpdesk for action. The account will then be disabled immediately, and all access rights removed. The account will remain on the network for 3 months after being disabled. The account will then be deleted however certain important emails may be retained if so required and requested by a Director.

11.3 Security Incident Handling

(a) We recognise the risk of an incident occurring involving [**CLIENT NAME**] IT systems and as such we have put in place the following IT security incident handling procedures.

(b) An IT Security Incident can be described as any situation involving Information Technology systems or information that is stored, manipulated or communicated by or through these systems being affected in an adverse way either through controlled or uncontrolled circumstances which could result in:

(i) loss, damage or theft of information;

(ii) disclosure of confidential information to unauthorised persons;

(iii) the integrity of IT systems or information being put at risk; and/or

(iv) availability of IT systems or information being put at risk.

(c) We recognise the importance of all IT related security incidents being handled using a structured, coherent and proven method, ensuring all incidents are handled in a consistent manner.

(d) All IT related incidents will be processed through the Director to ensure continuity on the handling of any incidents occurring.

(e) All IT security related incidents must be reported to both the Resman Helpdesk and to the Directors with immediate effect in the event of any such incident occurring. The Directors will liaise with the Resman Service Delivery Manager should there be an occurrence of any such incident.

11.4 Business Continuity

[**CLIENT NAME**] is aware that some form of disaster may occur, and as such, the Directors will implement and regularly update a business continuity management process to counteract interruptions to normal activity and to protect critical processes from the effects of failures or damage to vital services or facilities.

11.5 Training

We will endeavour to train or supply training to all staff on IT systems in use, to include security awareness relating to IT systems due to increasing security risks surrounding IT systems.

11.6 Duties and Responsibilities

(a) **Directors**

The Directors are the accountable officers responsible for the management of Information Management & Technology ("**IM&T**") Security and for ensuring appropriate mechanisms are in place to comply with Information Governance, IT Security and all current legislation.

(b) **Senior Staff**

It is the responsibility of all Directors to ensure that staff work within the boundaries of our policies and procedures and that staff are aware of their responsibilities.

(c) **All staff**

All employees of [**CLIENT NAME**], staff working in a voluntary capacity or independent contractors, must adhere to the current legislative framework and [**CLIENT NAME**] policies.

11.7 Monitoring and Compliance

The policy will be monitored for effectiveness by measurement of the number of reported IT security incidents reported.

12. Development & Consultation Process

12.1 The Policy has been developed by Resman Limited, our outsourced IT partner and has been reviewed and approved by a Director of Resman Limited.

12.2 This policy will be under continual development and consultation due to the nature of Information Technology and its constant evolvement with the introduction of new technologies. The policy will also be reviewed on an annual basis.

13. Reference Documents

ISO27001

https://www.iso.org/standard/54534.html

Data Protection Act 2018 (the '2018 Act') and the EU General Data Protection Regulation ('GDPR')

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

The Health & Safety at Work Act

http://www.opsi.gov.uk/si/si1995/Uksi_19950263_en_1.htm

The Freedom of Information Act

http://www.opsi.gov.uk/ACTS/acts2000/20000036.htm

The Computer Misuse Act

http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm

Copyright, Designs & Patents Act 1988

http://www.opsi.gov.uk/acts/acts1988/Ukpga_19880048_en_1.htm

The Human Rights Act 1998

http://www.opsi.gov.uk/ACTS/acts1998/19980042.htm

Electronic Communications Act 2000

http://www.opsi.gov.uk/acts/acts2000/20000007.htm

13.1 Computer Misuse Act 1990

For your information, the following activities are criminal offences under the Computer Misuse Act 1990:

(a) Unauthorised access to computer material i.e. hacking;

(b) Unauthorised modification of computer material; and

(c) Unauthorised access with intent to commit/facilitate the commission of further offences.