

## Information Security Policy

### Contents

	Page
1. Purpose	2
2. Applicability	2
3. Goals of this Policy	2
4. Responsibilities	3
5. Introduction	4
6. Policy Statement	4
7. Guidelines	5
7.1 General	5
7.2 Physical Security	5
7.3 Computer Security	6
7.4 Passwords	6
7.5 Backups	7
7.6 Network Shared Drives	7
7.7 Internet filtering	7
7.8 Wireless Access	8
7.9 Remote Access	9
7.10 Viruses	10
7.11 Network Accounts	10
7.12 Use of Electronic Mail	11
7.13 Use of the Internet	11
7.14 Manual Information Security	13
7.15 Mobile Workers and Home Workers	14
7.16 Incident Reporting	14
7.17 User's Responsibilities	14
7.18 Management Responsibilities	15
7.19 Controls	16
Appendix A Data Protection and Related Acts	17
Appendix B Security Checklists	19
Appendix C Security Incident Report	21
Appendix D Equipment Sign Out Sheet - IT Equipment Loan Agreement	24
Appendix E Internet filtering policy filtering	25
Appendix F Glossary	27

## Information Security Policy

### 1. Purpose

1.1 Information is a vital and valuable product of the Hereford & Worcester Fire and Rescue Service (HWFRS) activities and its community fire safety awareness strategies. Information systems are a critical resource in enabling these core activities and communicating work with our staff, citizens and business partners. The HWFRS recognises that global access to information provides many opportunities but also many challenges. The commercialisation of the internet has allowed an undesirable element of malicious hackers and virus writers to attack free and open networks. We are now dependent on a secure environment to undertake our core business and protection of our information systems and information assets is essential. This policy forms part of an overall Information Security Management System (ISMS) conforming to BS/ISO 27001 and will be built into the HWFRS management of risk framework at the highest level. It applies to all members of the HWFRS and those who use the Information and Communications Technology (ICT) infrastructure and associated information systems.

1.2 The implementation of this policy is important to maintain and demonstrate the integrity and security in the HWFRS.

1.3 It is the policy of the HWFRS to ensure:

- Information is protected against unauthorised access
- Confidentiality of information is maintained
- Information is not disclosed to unauthorised persons through deliberate or careless action
- The integrity of information through protection from unauthorised modification
- The availability of information to authorised users when needed
- Regulatory and legislative requirements will be met (Refer to Section 3 and Section 5.3 of this policy)
- Contingency plans will be produced and tested as far as is practicable to ensure business continuity is maintained
- Information security training will be given to all staff
- All breaches of information security and suspected weaknesses are reported, investigated and appropriate action is taken

### 2. Applicability

All HWFRS personnel and suppliers of goods and services, employed under any form of agreement, who have involvement with information assets covered by the scope of the ISMS, will be responsible for implementing this policy and shall have the support of the HWFRS who has approved this policy.

### 3. Goals of this Policy

3.1 To identify through appropriate risk assessment the value of information assets, to understand their vulnerabilities and the threats that may expose them to risk.

3.2 To manage the risks to an acceptable level through the design, implementation and maintenance of a formal Information Security Management System. To comply with legislation including:

- Data Protection Act
- Computer Misuse Act
- Regulation of Investigatory Powers Act
- Freedom of Information Act
- Access to Medical Records Act
- Human Rights Act

### **3.3 Specific Policies and Conditions**

Specific Service Policy/Instructions (SPIs) exist to support this document, including:

- IT User Guidelines
- Internet Acceptable Use

This list is not exhaustive and may be subject to additions or deletions to be approved by the HWFRS Management Team from time to time.

## **4. Responsibilities**

4.1 The HWFRS Principal Officers Management Team accepts and endorses this policy and is ultimately responsible and accountable for ensuring that the objectives of the security policy are met.

4.2 The Principal Officers Management Team will approve detailed policies and procedures for information security and agree the implementation arrangements.

4.3 The Head of ICT will be responsible to the Head of Asset Management for implementation of the policy and is authorised to pursue activities to achieve the policy objectives and for the creation and review of this policy and the underpinning Information Security Management System.

4.4 The ICT department in association with other IT and Communications staff are responsible for advising users on security issues, preventative monitoring of information systems and investigating security incidents.

4.5 All users of HWFRS information systems are responsible for protecting information assets. Users will at all times act in a responsible, professional, ethical and security conscious way, maintaining an awareness of and conformance with the security policy.

4.6 All personnel and contractors must follow all and any procedures in place, which are designed to maintain the Information Security Policy (ISP).

4.7 All personnel have a responsibility for reporting security incidents and any identified weaknesses. Users should report any breach in information security or suspected breach to the Head of ICT or IT Department staff.

4.8 Any deliberate act to jeopardise the security of information that is the property of The HWFRS or its clients will be subject to disciplinary and/or legal action as appropriate.

#### **4.9 Review**

This policy will be reviewed annually and in the case of any appropriate changes, amended to ensure it remains consistent for the HWFRS and its ability to serve its clients.

### **5. Introduction**

5.1 This policy aims to set out the HWFRS rules and procedures relating to information security and all staff responsibilities relating to information security.

5.2 The implementation of strict guidelines is a matter of great importance. Such guidelines must be considered together with the Organisations Information Security Policy and must be recognised by staff at all levels who must ensure they are applied at all times. They must also be supported by management who must take responsibility for their implementation and on going adherence.

5.3 This document should be read in conjunction with the SPIs and UK Law;

- British Standard for Information Security BS/ISO 27001
- Data Protection Act
- Computer Misuse Act

Any and all breaches of security covered by this policy must be reported to Senior Management and to the Head of ICT at the earliest opportunity.

### **6. Policy Statement**

6.1 It is the policy of the HWFRS to ensure that all information systems operated by the HWFRS are secure systems, which comply with the requirements of the Data Protection Act, the Computer Misuse Act and the British Standard for Information Security BS/ISO 27001. It is also the aim of the Organisation that its entire staff must be fully aware of the need to maintain secure systems and they must fully understand their responsibilities as outlined in this policy document.

6.2 Line Managers will be responsible for ensuring that their staff are aware of these procedures and their contents. They will also ensure that their staff abide by them.

6.3 Failure by any employee of the HWFRS to abide by the contents of this document will be viewed as a serious matter and may result in disciplinary action.

6.4 Responsibility for Data Confidentiality and Integrity for the various dedicated information systems lies with the individual Data Administrators.

6.5 All Security Incidents will be reported and managed by the Head of ICT.

## 7. Guidelines

### 7.1 General

7.1.1 Information security shall include protection of the following:

- Confidentiality: Ensuring that information and systems are accessible only to authorised users.
- Integrity: Safeguarding the accuracy and completeness of information and processing methods.
- Availability: Ensuring that authorised users have access to information and systems when needed.

7.1.2 This policy shall apply to:

- All information systems (including computer equipment, network equipment and telecommunications equipment) owned or operated by the HWFRS or connected to the network.
- All software (including operating systems, network services and application software) installed on applicable information systems.
- All information stored on the relevant information systems.

### 7.2 Physical Security

7.2.1 System users, Department Heads and Officers in Charge have responsibility for the physical security of equipment in their care and should take appropriate precautions.

7.2.2 Equipment at risk may be fitted with security locks or alarms if appropriate in the circumstances, by the Information Technology Department.

7.2.3 Do not, under any circumstances, leave a laptop/notebook computer or any other valuables unattended.

7.2.4 Theft, damage or loss of equipment must be reported immediately to the appropriate Line Manager. The individual must also report the loss to the ICT department on the next working day and make a report to the Police within 24 hours of the incident. A report of the incident must be filed with the Head of Asset Management within 2 weeks of the incident taking place.

7.2.5 Access to data held on HWFRS information systems can be minimised by restricting physical access to HWFRS buildings.

7.2.6 Where information is kept in offices access to buildings must be restricted. Such restrictions include making sure security doors are closed properly and that manual entry codes are changed regularly.

7.2.7 All doors and windows must be appropriately secured at all times.

7.2.8 Visitors to HWFRS buildings must be accompanied at all times and signed in and out of the premises on arrival and departure.

## 7.3 Computer Security

7.3.1 We are responsible for any data we enter on our computers. The very nature of the type of information we are dealing with makes protection of that information of prime importance.

7.3.2 We have legal responsibilities under the Data Protection Act and the Computer Misuse Act to ensure that unauthorised access to our data is not permitted and also that data is accurate and kept up to date. Such restrictions apply not only to people outside the organisation but may also apply to those in the organisation whose work does not necessitate access to the data. All staff must abide by the rules of the Data Protection Act and the Computer Misuse Act and also any guidelines, which may be issued from time to time.

7.3.3 Never leave your computer unattended when it is logged on. Whenever you move away from your workstation ensure you log off or lock your workstation. IT has a policy in place to automatically lock workstations after a pre-determined period of time has expired. Under no circumstances are users to rely of this facility to lock workstations in their absence.

7.3.4 Always ensure, when leaving your place of work, to log off and close down your workstation correctly.

7.3.5 You must not download and/or install software onto HWFRS systems unless specifically authorized to do so, that software has been approved and you can validate that it is licensed for current use within the HWFRS.

7.3.6 Computers that use their own modems to create independent data connections side-step the network security mechanisms. An individual connection to any outside computer could be used by an attacker to compromise any HWFRS network to which that computer is connected. For this reason, any computer used for independent dial-up or leased-line connections to any outside computer or network must be physically isolated from HWFRS internal networks, unless the connections have been specifically authorised by the ICT department. Connections to the Internet using modems from network-connected computers are specifically prohibited.

7.3.7 The loan, movement or reconfiguration of all/any ICT equipment must NOT occur without the express approval of the Head of Asset Management, or Head of ICT. The only exception to movement is those users allocated laptops or mobile devices which by their nature are intended for mobile use.

## 7.4 Passwords

7.4.1 Most systems within the HWFRS require a log in name and password for access. All staff are given access rights and privileges to the various systems in accordance with the area in which they are working and the type of data they require to use. All staff will have a log-in for one or more of the network servers in addition to any other systems they use.

7.4.2 In all cases any passwords given to you personally are for your use only. Passwords should not be written down or given to others to use under any circumstances.

7.4.3 Passwords should be a minimum of 6 characters and should be a combination of letters and numbers and at least one uppercase letter.

7.4.4 To make the accidental discovery of passwords more difficult, do not use family or pet names and if at all possible try not to use proper words.

7.4.5 Passwords must be changed on a regular basis. The HWFRS policy is every 42 days. Some systems will prompt for this, others do not. If they do not it is your responsibility to change them. If you suspect someone else may have detected your password or you suspect someone else is using it, you must change your password immediately and advise your Manager.

## **7.5 Backups**

7.5.1 The IT department will ensure servers and the files contained thereon are backed up on a daily basis.

7.5.2 It is the responsibility of individual users to back up any systems, which do not deposit their data centrally.

7.5.3 All backups must be kept up to date and must be checked on a regular basis to ensure that it is possible to recover the data on them.

## **7.6 Network Shared Drives**

7.6.1 It is the policy of the HWFRS to keep all of its data in a secure manner and to only allow authorised access to files to those who require the data as part of their normal duties. Unless there are specific reasons not to do so, all data files will be saved on the network file servers and NOT on local PCs.

7.6.2 The ICT Department will grant access to individual data areas as requested in writing by the “owners” of that area. Additionally, Managers and Supervisors will have access to their staff’s individual areas if required.

7.6.3 It is expected that users will make all files of general interest available (normally read only) on a suitable location on the server(s).

7.6.4 Each user is assigned their individual storage area. Only you have access to the files in this area unless you specifically ask the service Help Desk to grant access to others.

## **7.7 Internet Filtering**

7.7.8 Internet filtering (blocking/unblocking) of individual web sites or general classes of sites will be instituted for the following reasons:

- a) ICT Management Request. ICT Management can request a web site or class of sites be blocked based on an analysis of web site access for the following reasons:

- network performance,
- an apparent violation of existing law and/or policy,
- Perceived security risks.
- Distraction to normal working practices

b) Departmental Request. A department can request a site or class of sites be blocked/unblocked for a single device, group of devices or all of the devices in a department. Departments must make requests for blocking/unblocking in writing to the Head of ICT.

7.7.22 The sites or classes of sites filtered, is subject to change at any time. ICT will notify users of the HWFRS Internet services prior to the implementation of a filter, unless it is deemed to be an emergency.

7.7.23 Departments that have particular devices that need access to unblocked sites can request that access be provided specifically to them. Department requests must be received from the department head. The request should be directed to the Head of ICT.

7.7.24 A list of web sites filtered is contained in Appendix E. An up to date list is available on the ICT intranet web site.

## 7.8 Wireless Access

7.8.1 Access to the HWFRSNet requires user authentication and access based on Wireless Protected Access (WPA) and port based certificate management providing strong encryption.

7.8.2 Users accessing a wireless Access Point (AP) must have approval from their Line Manager.

7.8.3 The Head of ICT reserves the right to disallow wireless access to the HWFRSNet if that access would result or is resulting, in a degradation of service to other users or for reasons of security.

7.8.4 Hosts will be configured to connect to APs. Host to host (ad hoc) connections are not permitted.

7.8.5 Authorised users may at any time be removed from the list of authorised users if their access is considered a risk to security or it is deemed that access is being used in an inappropriate manner. Access will be removed by the revocation of the user's certificates.

7.8.6 APs may need to be shut down or reconfigured at any time, if another device in the area experiences or is the source of interference in the relevant frequency ranges.

7.8.7 IP numbers allocated by an AP will be allocated dynamically as allocated by the IT Department.

7.8.8 IT will be responsible for installing root and user certificates on each host requiring wireless access and ensuring adequate security measures are in place for securing the HWFRSNet network and protecting sensitive information.

7.8.9 Records of access will be retained for at least 60 days. Logs will include the identity of the user, IP address and the date and time of the connection.

## 7.9 Remote Access

7.9.1 It is the responsibility of HWFRS employees, contractors, vendors and agents with remote access privileges to the HWFRSNet network to ensure that their remote access connection is given the same consideration as the user's on-site connection to the HWFRSNet.

7.9.2 General access to the Internet for recreational use by immediate household members through the HWFRSNet Network on personal computers is permitted for employees that have flat-rate services. The HWFRS employee is responsible to ensure the family member does not violate any the HWFRS policies, does not perform illegal activities and does not use the access for outside business interests. The HWFRS employee bears responsibility for the consequences should the access be misused.

7.9.3 Please review the following documents for details of protecting information when accessing the corporate network via remote access methods and acceptable use of the HWFRSNet network:

- a) *Information Security Policy (ISP) Guidelines (This document)*
- b) *Data Protection guidelines*
- c) *Computer Misuse Act*

7.9.4 For additional information regarding remote access connection options, including how to order or disconnect service, cost comparisons, troubleshooting, etc., view the intranet web site <http://web/hwfirenet> or contact the IT helpdesk or telephone 01905 368444.

7.9.5 Secure remote access must be strictly controlled. Control will be enforced via authentication, public/private keys with strong pass-phrases and/or certificate based authentication. For information on creating a strong password refer to the Password Guidelines located within the Information Security Policy.

7.9.6 At no time should any HWFRS employee provide their login or email password to anyone, not even family members.

7.9.7 Employees and contractors with remote access privileges must ensure that their HWFRS owned or personal computer or workstation, which is remotely connected to the HWFRSNet corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.

7.9.8 HWFRS employees and contractors with remote access privileges to the corporate network must not use non-HWFRS email accounts (i.e., Hotmail, Yahoo, AOL) or other external resources to conduct corporate business, thereby ensuring that official business is never confused with personal business.

7.9.9 Routers for dedicated Integrated Services Digital Network (ISDN) lines configured for access to the HWFRS network must meet minimum authentication requirements of Challenge Handshake Access Protocol (CHAP).

7.9.10 Reconfiguration of a home user's equipment for the purpose of split-tunnelling or dual homing is not permitted at any time.

7.9.11 Non-standard hardware configurations and security configurations for access to hardware must be approved by the Head of ICT.

7.9.12 All hosts that are connected to the HWFRS internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers. Third party connections must comply with HWFRS requirements as defined by the ICT department.

7.9.13 Personal equipment that is used to connect to the HWFRS network must meet the requirements of the HWFRS owned equipment for remote access.

7.9.14 Organisations or individuals who wish to implement non-standard Remote Access solutions to the HWFRS production network must obtain prior approval from the Head of ICT.

## **7.10 Viruses**

7.10.1 It is the responsibility of all staff to protect HWFRS computer systems from viruses. All files received on disc from outside the HWFRS (including those used on home PCs) and any received via electronic mail must be checked for viruses before being used.

7.10.2 All staff will be instructed in the use of anti virus software and must ensure that all discs are virus checked whatever their source.

7.10.3 If you receive any e-mails that you are unsure of or you do not recognise the sender then do not open them. If you are unsure, inform the HWFRS Help Desk and your Manager.

7.10.4 If a virus is suspected, the ICT HWFRS Help Desk should be informed immediately. The workstation should not be used and a sign stating this should be placed on the workstation to warn other users until given permission from ICT to reuse the equipment is obtained. Any disks or CD ROMS that have been used on the suspected infected workstation should be gathered together and not used.

## **7.11 Network Accounts**

7.11.1 The ICT HWFRS Help Desk is responsible for the issue of Network Log on accounts and email accounts.

7.11.2 Data Administrator's are responsible for allocating access rights to staff wishing to access their systems. Where it is only possible for the IT HWFRS desk to issue log on accounts, then procedure as shown in specific System Security Policies must be followed.

7.11.3 All access to internal systems via remote connections must be authorised by a Principle Officer and be in accordance with all relevant UK and European Legislation. All connections will be provided subject to service availability and capacity. All connections will be governed by an access agreement.

## 7.12 Use of Electronic Mail

7.12.1 All staff should be aware of the procedures relating to e-mail use as detailed in the 'IT User Guidelines Policy'.

7.12.2 Data sent electronically by e-mail is not secure unless encrypted and the HWFRS has not yet implemented a universal system to achieve this. **You must not send personal data or identifiable information by e-mail.**

7.12.3 Staff are forbidden to create copy, store, transmit, view, display or download messages or material from whatever source that may put the HWFRS at risk of prosecution, civil action, embarrassment or loss of reputation. This includes defamatory, obscene, discriminatory or abusive or otherwise inflammatory messages.

7.12.4 E-mails with the following content must not be sent;

- Sexually explicit text or images
- Discriminatory text or images including on grounds of race, religion, national origin, ethnic origin, sex, sexual orientation and physical or mental ability
- Jokes or chain letters
- Text or images of a violent nature
- Text or images support criminal acts
- Gambling
- Text or images relating to private or freelance business

7.12.5 If you receive any of the above e-mails you must notify your Line Manager immediately.

## 7.13 Use of the Internet

7.13.1 Users will be expected to refrain from using the Internet for the following:

- Any activity which does not comply with existing HWFRS policy;
- Display of any kind of sexually explicit, pornographic, obscene or offensive material;
- Knowingly committing an illegal act;
- Compromising the integrity of the network;
- Making unauthorised contact with outside bodies;

- Downloading or playing games;
- Making available to others (uploading) HWFRS owned software;
- Using personal modems on network-connected workstations.

7.13.2 Internet access provided by the HWFRS must only be used for HWFRS business related activities. It is not permitted for any individual to use the HWFRS Internet connection for personal use. Limited use of facilities in the development of professional knowledge and maintenance of professional contacts is permitted. Specifically users must not access any websites, chat rooms or news groups that are known as or could be suspected of, containing illegal, objectionable, defamatory, obscene, discriminatory or otherwise inflammatory material.

7.13.3 In particular, any employee who is found to have visited pornographic or abusive websites or to have received and then retained and/or transmitted pornographic or abusive material will be subject to disciplinary proceedings, which may result in summary dismissal.

7.13.4 Staff must not download, copy, store or transmit material using HWFRS systems that may violate copyright, trademark, trade secret or other license restrictions.

7.13.5 All users should be aware that Internet access is monitored centrally and any deliberate access of unacceptable sites may result in notification to the appropriate Line Manager and possible disciplinary action.

7.13.6 ICT has software systems in place to monitor and record all Internet usage. These security systems are capable of recording (for each and every user) each World Wide Web site visit, each email message and each file transfer into and out of our internal network and we reserve the right to do so at any time. The HWFRS may review Internet activity and analyse usage patterns and may choose to publicise this data to ensure that Internet resources are devoted to maintaining the highest levels of productivity.

7.13.7 The HWFRS reserves the right to inspect any and all files stored in user defined areas of its network in order to ensure compliance with policy.

7.13.8 The display of any kind of sexually explicit image or document on any HWFRS system is a violation of HWFRS policy and will result in a disciplinary investigation. In addition, sexually explicit material may not be archived, stored, distributed, edited or recorded using the HWFRS network or computing resources.

7.13.9 If personnel find themselves connected accidentally to a site that contains sexually explicit or offensive material, they must disconnect immediately, regardless of whether that site had been previously deemed acceptable by any screening or rating program. To disconnect quickly from a site, use the "Home" button on your web browser.

7.13.10 The HWFRS's Internet facilities and computing resources must not be used to knowingly commit an illegal act. Use of the HWFRS resources for illegal activity will result in disciplinary action, which may lead to dismissal.

7.13.11 Personnel with Internet access must only download software with direct business use and must arrange to have such software properly licensed and registered through the IT Department where required. Downloaded software may only be used under the terms of its licence and only if authorised by the IT Department (Note: Adobe Acrobat is already authorised by them). Any software or files downloaded via the Internet into the HWFRS network become the property of the HWFRS.

7.13.12 Personnel must not use the HWFRS facilities to knowingly download or distribute pirated software or data.

7.13.13 Personnel must not use the HWFRS facilities to deliberately propagate any virus, worm, Trojan horse or trap-door program code.

7.13.14 Personnel must not use the HWFRS Internet facilities to knowingly disable or overload any computer system or network or to circumvent the security of another user.

7.13.15 Personnel shall identify themselves honestly, accurately and completely (including their HWFRS affiliation and function where requested) in all Internet activity.

7.13.16 The HWFRS retains the copyright to any original material posted on the Internet by any employee in the course of their duties.

7.13.17 Personnel are reminded that the Internet is a public forum where it is inappropriate to reveal confidential HWFRS information or data. Personnel releasing such information will be subject to disciplinary action.

7.13.18 Use of HWFRS Internet facilities to commit acts such as misuse of HWFRS assets or resources, sexual harassment, unauthorised public speaking and misappropriation or theft of intellectual property will result in disciplinary action.

7.13.19 Personnel must not use HWFRS Internet facilities to download entertainment software or games or to play games individually or against opponents over the Internet.

7.13.20 Personnel must not copy any HWFRS licensed software to anyone else without specific authorisation.

7.13.21 The HWFRS has installed a *'firewall'* to ensure the safety and integrity of the HWFRS networks. Additional devices may also be installed in the future to further protect these networks. Personnel must not attempt to disable, defeat or circumvent any security facility.

## **7.14 Manual Information Security**

7.14.1 A "clear desk policy" will be operated throughout the HWFRS. All manual files and paper records should be locked away before leaving the office. Where this is not possible or where offices employ "open" shelving for the storage of files and documents, offices must be locked at all times when left unattended.

7.14.2 Confidential waste shall be disposed of securely. Confidential waste shall be shredded or placed in the appropriate containers for secure disposal.

7.14.3 All confidential information shall be held securely in locked containers, lockers, drawers and filing cabinets to prevent unauthorised access

## **7.15 Mobile Workers and Home Workers**

7.15.1 Any portable computing equipment must not be left unattended unless it is protected by a security device. Security devices could include locking an office door, keeping the equipment in a restricted access area or a physical lock securing the equipment to the desk.

7.15.2 The employee's Line Manager must be informed of any sensitive personal data that is removed from HWFRS premises and a record made of that removal.

7.15.3 All portable equipment or equipment not permanently allocated to the employee and taken for use off HWFRS premises must be signed for by the member of staff concerned.

7.15.4 Portable computer equipment containing personal files shall only be removed from HWFRS premises where absolutely necessary. If personal data is used off site then wherever possible the equipment shall be returned to HWFRS premises immediately after use.

7.15.5 When laptops are used, users are to ensure that they require a user log on and password and they have a physical encryption key. The IT department will provide a encrypted and password secured folder area on the laptop where all sensitive data must reside. Where manual files are processed outside of HWFRS property they should be kept with the data processor wherever possible. When left unattended they should be in a locked container and out of view.

7.15.6 Any computer equipment or manual files that are travelling with an employee must be locked in the boot of the car. Under no circumstances should any computer equipment or manual files be left unattended and externally visible in a vehicle at any time.

## **7.16 Incident Reporting**

Any breaches of security, however minor, must be reported to the Head of ICT who shall use ITC1 Form (Appendix C) to record the incident.

## **7.17 User's Responsibilities**

7.17.1 Each individual must ensure that as far as is possible no unauthorised person has access to any data held by the Organisation. Each person must ensure that any physical security measures are properly used.

7.17.2 Individuals must not deliberately or negligently corrupt, damage or destroy data, software or hardware belonging to the HWFRS. This includes the spreading of viruses or other similar computer programmes.

7.17.3 Individuals will be given access passwords to certain computer systems. These must not be disclosed to other members of staff. They should not be written down and they should be changed regularly.

7.17.4 Staff must not load software packages onto their PCs. This must only be carried out by HWFRS IT staff. On no account must games software be loaded on staff PCs.

7.17.5 Any files received on removable media brought or sent into the Organisation or files received electronically must be virus checked before being loaded onto an Organisation PC. This includes disks which have been used on machines at home or otherwise not on HWFRS premises. Never leave your computer unattended when it is logged on. Whenever you move away from your workstation ensure you log off or lock your workstation.

7.17.6 If you cease to be employed by the HWFRS, you must return all computer files, including those on removable media, plus all software and hardware to your Manager.

7.17.7 A security checklist covering these responsibilities is given in Appendix D. All staff must be provided with a copy as a reminder of their responsibilities.

## **7.18 Management Responsibilities**

7.18.1 Line Managers and Directors must give their full backing to all the guidelines and procedures as set out and agreed in this document.

7.18.2 Managers, where they have responsibility for individual systems, must maintain records of users of that system and control their access to it by the granting of access privileges, passwords etc. They must:

- check the user has authorisation to use the service
- check the level of access is appropriate for the business purpose and is consistent with this security policy
- maintain a formal record of all registered users
- immediately remove access rights of users who have left the Department or the HWFRS
- periodically check for and remove redundant users accounts from the system
- ensure redundant user accounts are not re-issued to new users.

7.18.3 Where the granting of user access can only be carried out by the IT HWFRS Help Desk, the Manager must still fulfil the above and advise the IT HWFRS desk.

7.18.4 Line Managers must make the ICT HWFRS Help Desk aware of all new staff and leaving staff so that log-in rights and access privileges can be set or removed as appropriate. They must also issue staff leaving with a written reminder that they continue to be bound by their signed confidentiality agreement.

7.18.5 Where staff do not have sufficient knowledge to be able to use systems efficiently and securely their Managers must ensure that appropriate training is arranged before allowing them access to the Organisation's computer systems.

7.18.6 Managers must also take responsibility to ensure:

- all staff receive a briefing on the Data Protection Act as part of their induction programme within two weeks of joining the Organisation
- all staff are aware of the strict confidentiality of the information to which they will have access
- staff use the information in an appropriate manner at all times.

7.18.7 A more detailed explanation of these responsibilities is given in Appendix C. All staff must be provided with a copy as a reminder of their responsibilities.

## 7.19 Controls

7.19.1 It is up to all staff who have responsibility for others in the organisation to ensure that these individuals adhere to these procedures.

7.19.2 The ICT Department will be responsible for monitoring systems under their control for signs of:

- Illegal or unauthorised software having been loaded
- Password misuse
- Unauthorised access.

7.19.3 Spot checks will also be made to ensure that where data is not held and backed up centrally, adequate backups are being made.

7.19.4 All breaches of I.T. security will be reported to the Departmental Head of the member of staff concerned and may be used as the basis of a disciplinary action. A copy of the Security Incident Report is included at Appendix D.

7.19.5 The Organisation's internal audit staff will regularly review the Organisation's performance in implementing this policy.

## Appendix A

### Data Protection and Related Acts

#### Data Protection Act 1998

1. This Organisation is currently registered under the Data Protection Act. Staff must be aware of their responsibilities under this Act.
2. The Act outlines how data should be obtained, stored, maintained and disposed of. It also sets out details of our responsibilities to data subjects.
3. All staff must have the terms of the Data Protection Act fully explained to them within two weeks of joining the Service. There will be regular update sessions organised by Corporate Risk to ensure continued adherence to the Act.
4. There are a set of eight principles (listed below) which all staff should be aware of and which should be adhered to closely:
  - a) **Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless: - at least one of the conditions in Schedule 2 is met, and in the case of sensitive personal data, at least one of the conditions in schedule 3 is also met.**
  - b) Processing includes collection of data. Reference to Schedule 2 and 3 refer to conditions under which data can be processed.
  - c) These conditions cover such reasons as Legal Obligation, Protection of the Data Subject and for legal or medical purposes. However the safest reason would be the consent of the data subject.
  - d) **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.**
  - e) Any changes in the purpose for which data are obtained or held must be notified to the Data Protection Officer who will arrange for an amendment to the notification. It is important that all users familiarise themselves with the notification to ensure compliance with this principle.
  - f) **Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.**
  - g) Data should not be held “in case we might need it later”. It must be held for a specific reason and must all be relevant.
  - h) **Personal data shall be accurate and where necessary kept up to date.**
  - i) Any changes which affect the data must be made as soon as possible.
  - j) **Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes.**

- 
- k) Once the specific task for which the data is required is completed the data must be erased.
- l) **Personal data shall be processed in accordance with the rights of data subjects under this Act.**
- m) This refers to a data subject's right of access to information held about them.
- n) **Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of or damage to, personal data.**
- o) This covers physical and technological security measures as regard losses and unauthorised amendment and deletion of data also the "fire and flood" preventative measures which must be in place.
- p) **Personal data shall not be transferred to a county or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.** There are some exceptions to this which are detailed in the Act.

## Subject Access

Data subject access requests should be dealt with in accordance with HWFRS Subject Access Request Policy.

## Computer Misuse Act 1990

This sets out guidelines relating to the use and misuse of computers and gives employers a course of action against staff who use computers in a manner not considered appropriate to their terms of employment.

The act introduced three new criminal offences of:

- unauthorised access
- unauthorised access with intent to commit a further serious offence and
- unauthorised modification of computer material.

This Act ties in with the Data Protection Act in relation to the protection of data in general.

## Appendix B

### Security Checklists

#### Computer Users Security Responsibilities

**If you use a HWFRS computer system then you have the following responsibilities.**

You will have a log on account which is unique to you and which you must not let anyone else use.

You will maintain a password as set out below which you will not allow anyone else to use. (Access to other people's data through your own account can be arranged through the IT service Desk.)

- In all cases any passwords given to you personally are for your use only. Passwords should not be written down or given to others under any circumstances.
- Passwords must be a minimum of 6 characters and should be a mixture of letters and numbers.
- Do not use family or pet names or other easily guessed words and if at all possible try not to use proper words. This makes the accidental discovery of a password more difficult.
- Your passwords must be changed on a regular basis. The HWFRS policy is every 42 days. Some systems will prompt for this, others do not. If they do not it is your responsibility to change them.

You must report any suspected tampering with your log-on accounts to your head of department.

You must not load any private programs or games onto any of the computers.

You must not load any other software (other than data) without the express permission of the IT service Help Desk.

No unauthorised private work/projects are to be carried out on the Organisation's PC's

All data disks and all files from any source (including e-mail) must be virus checked prior to being used.

All data to which you have access during the course of your work is to be treated in strict confidence and its accuracy must be maintained.

You must not access information unless your job specifically requires it.

You must abide by the terms of the Data Protection Act 1998 and the Computer Misuse Act 1990.

Do not store identifiable or other confidential data on portable PCs, which are taken out of the office and therefore represent an increased security risk.

---

Do not use any of the Organisation's Computer Systems for accessing any sites or functions (including email) of the HWFRS or Internet other than to strictly fulfil the requirements of your job.

**Failure to carry out these responsibilities will be treated as a serious matter and may result in disciplinary action.**

### **Line Manager's Security Responsibilities**

**As a Line Manager responsible for other staff you have the following responsibilities in addition to those you have as a user.**

You must maintain a record of the access rights your staff have.

You must notify the IT service desk or the Manager responsible for particular computer systems of any changes of staff (i.e. joiners and leavers) and what levels of access you require your staff to have to the various systems.

You must notify the IT service desk of any starters and leavers and also issue any leavers with a written reminder that they continue to be bound by their signed confidentiality agreement.

You must ensure that all your staff are aware of their responsibilities and that they carry them out. Any breaches must be treated as serious and be reported to the Head of Information Systems and/or to the Head of Human Resources.

You must only provide staff with the minimum access required to carry out their duties.

You must ensure that all your staff are aware of their responsibilities and have the appropriate training before they are allowed access to the Organisation's computer systems.

You must set an example to all your staff in your conduct and attitude towards computer use and security.

**Failure to carry out these responsibilities will be treated as a serious matter and may result in disciplinary action.**

### **Director's and Senior Manager's Security Responsibilities**

As a Director/Principal Officer or Senior Manager in addition to your responsibilities as a computer and a Line Manager user you must also:

Ensure that your Line Managers are implementing this security policy.

Set an example to all your staff in your conduct and attitude towards computer use and security.

**Failure to carry out these responsibilities will be treated as a serious matter and may result in disciplinary action.**

## Appendix C

### Security Incident Report

These notes accompany and form part of the HWFRS ICT1 – Security Incident Report Form. This Form is intended for use by all Departments served by the HWFRS.

#### Definition of Security Incident

A security incident is defined as:

“Any unplanned or unforeseen event which has the capability of causing disruption to the operation of the organisation or which by its happening has the potential to cause a security breach by disclosing, deliberately or accidentally data or information under the control of the organisation”.

Such events may include but are not limited to:

- Virus infection (either single machine or file or of the whole network).
- Password abuse (either by deliberate use or sharing of another user’s password or by attempting to gain access to the system by hacking).
- Loss or theft of equipment, which may contain patient or other confidential data at risk of disclosure.
- Deliberate or accidental disclosure of confidential data.

#### Action to be taken on identifying an “Incident”

The person discovering the incident must complete Section 1 of ICT1 Form, making sure that any immediate actions to minimise the effects of the incident are recorded.

The person above must notify their Line Manager that an incident has occurred and the Line Manager must make an initial assessment of the severity of the incident.

A copy of the Form should then be sent immediately to the Head of Information & Communications Technology (Head of ICT), (preferably by email) with a signed hard copy to follow.

If the incident is considered serious, then the Head of ICT or a member of the Information Technology Team must be notified by telephone straight away so that any immediate action taken can be discussed and its suitability assessed.

The Head of ICT (or his team) will assess the nature of the incident and consider what recommendations can be made.

## Appendix C

### ICT1 – SECURITY INCIDENT REPORT

A copy of this Form must be completed for all identified security incidents (Refer to attached for definition of incident). The Head of Information & Communications Technology is responsible for keeping copies of all Forms on file for later review by the Organisation's Auditors. All Security Incident Reports must be treated as management-in-confidence.

**Section 1: To be completed by person identifying the incident**

<b>Date/Time of incident:</b>	<b>Incident identified by:</b>	<b>Internal severity Classification: (See Attached)</b>
<b>Location of incident:</b>	<b>Name of organisation/dept of involved staff:</b>	
<b>Description of incident:</b>		
<b>Any immediate action taken:</b>	<b>Signed:</b>	

**Section 2: To be completed by the Head of Information & Communications Technology**

<b>Date/Time notified of incident:</b>	<b>Principal Officer / Director notified: (With immediate recommendation)</b>
<b>Proposed Action Plan:</b>	
<b>Signed:</b>	

**Section 3: To be completed by the IT Manager**

*(ICT will only be asked to comment if the Incident is one relating to matters under his control e.g. access or password violations or virus attacks)*

<b>Date/Time notified of incident:</b>
<b>Proposed Action Plan:</b>
<b>Signed:</b>

---

## Notes on Completion of and Actions relating to, Incident Report Form

### Internal Severity Classification

1. Actual data loss or abuse
2. Potential for data loss or abuse
3. Systems unavailable for use

### Data Categories (for use with 1 and 2 above)

- A. Personal information identifying an individual
- B. Financial Information
- C. HWFRS in confidence information
- D. Commercial in confidence information
- E. General Organisation information

Once an incident has been identified Section 1 of ICT1 Form must be completed and a Line Manager informed of the incident.

If the incident is considered as serious, the Head of ICT or a member of the Information Technology Team must be notified immediately by telephone so that any immediate actions can be discussed and agreed on.

It may be considered at this time that the incident is serious enough that the Chief Fire Officer (CFO) should be informed of the incident. The Line Manager to whom the incident is reported will be responsible for doing this, possibly after discussion with the Information Technology Team.

The incident report with Section 1 completed should then be forwarded to the Head of ICT.

The Head of ICT will complete Section 2 of the Form and advise what action should be taken. This advice may be a recommendation to investigate further or may constitute a more detailed action plan.

If the incident is one which involves a technical breach or which requires a technical solution (installation of AV software for example), the IT Manager will be asked to complete Section 3 of the Form with his recommendations or action plan.

If at any stage the investigation reveals that the incident is of a more serious nature than first identified or in any event once all the recommendations have been made, the CFO (or nominated security representative) must be contacted and any proposed action discussed with them.

Following completion of the Form and production of action plan a copy of the Form and plan must be retained by Head of ICT.

Appendix D

**ICT2 – Equipment Sign Out Sheet**

**IT Equipment Loan Agreement**

Permission is granted for the loan of the following equipment:

.....  
(description)

.....  
(name of person equipment loaned to)

**Subject to the following terms and conditions:**

All equipment must be ‘signed out’ by the borrower and authorised by a member of the HWFRS ICT Department.

The equipment is to be used by HWFRS employees for work purposes only.

The equipment must not be left unattended while in transit from work to your home or vice-versa: i.e. left on the backseat of your car. Loss or damage to the equipment through negligence on the part of the borrower may result in the borrower bearing the cost of any repair or replacement.

It is the responsibility of the **Borrower** to return equipment to the HWFRS ICT Service Help Desk and ensure that it is ‘signed in’. On **no account** is returned equipment to be left with the ICT service Help Desk without a ‘received signature’ **or passed on to another employee.**

The borrower agrees to take good care of the equipment.

All work taken off-site, which is of a confidential nature or identifies individuals and/or staff must be stored securely and every step taken to ensure that such information is not inadvertently disclosed to any third parties.

All terms of the HWFRS Information Security Policy apply to the use of this equipment.

I have both read and agreed to the above terms and conditions.

Borrower Signature :.....

Dept.:..... Date:.....

Authorised By :.....

Signature :..... Date:.....

## Appendix E

### INTERNET FILTERING POLICY WEB SITE FILTERS “Unauthenticated IPs”and “InetUsrGp0” groups

(Currently all HWFRS Users) – Last Update: November 2007

This appendix identifies the individual and classes of web sites filtered by the HWFRS. The sites or classes of sites filtered are subject to change at any time on request and with the approval of Management in consultation with the Head of ICT.

#### BANNED SITES

- Kazaa
- eDonkey
- Gnutella
- DirectConnect
- BitTorrent
- Ebay
- Facebook
- myspace

#### URL CLASSES

- Instant Messenger
- Chat sites
- Peer to peer (P2P)
- Adult
- Sexually Explicit Material (pornography)
- Web proxy or anonymous sites
- Virus infected sites
- Audio-video
- Dating
- Adware/Spyware

#### CONTENT FILTERING CLASSES

- Instant Messenger
- Chat sites
- Sexually Explicit Material (pornography)
- Games
- Drugs
- Hacking
- Gambling
- Peer to peer (P2P)

#### FILE EXTENSION CATEGORY BLOCKING CLASSES

- Archive (.zip, .tar, etc)
- In page executables (.exe, .com, .dll)
- Video (.avi, .mpg, .mov)
- Audio (.wav, .au, .mp3)
- Macros (.mdb)

### **MIME TYPE CATEGORY BLOCKING CLASSES**

- Archive (includes zip files)
- In page executables (Includes Java and Javascript)
- Octet (Includes any other binary file such as Word documents. These would not normally be files designed for web pages.)
- Audio (Includes wave files and similar)
- Messenger
- Video (Includes avi files and similar)

### **SERVICES ALLOWED (SOURCE RULES)**

- File Transport Protocol (FTP)
- Network News Transport Protocol (NNTP)
- Domain Name Service (DNS)
- HyperText Transport Protocol (HTTP)
- Secure HTTP (HTTPS)
- Post Office Protocol v3 (POP3)
- POP3 over Secure Socket Layer (SSL)
- Internet Meaasge Access Protocol (IMAP) over SSL

### **CONTENT REPLACEMENT CATEGORY BLOCKING**

- ActiveX
- All popups
- Blink
- Jshtml cookies
- On unload popups
- Web bugs
- Address bar spoofing
- Applets
- Cross site scripting
- Nimda worm
- Un solicited popups
- Windows moving scripts

## Appendix F

### Glossary

#### AV

Audio Visual

#### BS27001, ISO 27001

Framework of standards that provide a template for the creation of an Information Security Management System.

#### CHAP

Challenge Handshake Authentication Protocol is a way of authenticating users when they log on to a service.

#### Data Subject

Any individual implicated in data held by the Service

#### Firewall

A network security device used to protect private networks against Internet abuse from unknown origins.

#### Information Security Management System (ISMS)

Information System based on BS/ISO 27001 template enabling organisations to manage their information systems by identifying assets and associated risk in order to minimise those risks.

#### Network Shared drives

Method of file storage on a remote server or workstation.

#### Split tunnelling

A method of connecting to more than one network at a time.

#### SPI

Service Policy Instructions

#### Wireless Protected Access (WPA)

A form of protecting wireless access to network services by way of strong password authentication.