

Committee: FINANCE AND RESOURCES

Date: 9 May 2008

Report: INFORMATION TECHNOLOGY (IT) POLICY AND PROCEDURES

Purpose of the Report

1. To seek members' approval of the revised IT Policy and accompanying Procedures..

Strategic Planning Framework

2. The information and recommendations contained in this report are consistent with the Authority's statutory purposes and its approved strategic planning framework, and in particular its objective 'to manage all aspects of the Authority's business so as to make the most effective use of our resources' (Corporate Plan).

Background

3. In preparing the Information and Communications Technology (ICT) Strategy, the opportunity was taken to review and update the Authority's IT policies (now combined as one policy) and related procedures (please see **Appendix**). This Policy (and the related Procedures) is intended to assure the appropriate working of the IT system, and to ensure that officers operate the systems and services provided in an appropriate manner. As with the IT Strategy, the IT Working Group provided comments and amendments to draft versions of this work, as did appropriate professional officers (the Solicitor and the Personnel & Training Officer).

IT Policy and Procedures

4. The revised suite of policy and procedures is structured as follows:

- IT Policies & procedures ...the 'lead' document, which puts all the others into context. Effectively, the index for this policy suite. (**Appendix**)
 - Information Security (a new policy area; **Annex 1**)
 - Software Management (a new policy area; **Annex 2**)
 - Internet Acceptable Use.(**Annex 3**)
 - Remote Access Procedure (**Annex 4**). The Remote Access Policy is not included here. The latter deals with such issues as permission to work away from the office

and health & safety considerations, and was approved by this committee in 2006; it sits within the suite of personnel policies maintained on the Intranet.

- Email procedures and protocols (**Annex 5**)
- Back-Up procedure (new; **Annex 6**)
- Disaster recovery procedure (new; **Annex 7**)

5. The policy content within the above sections are all in line with current IT best practice.

6. The Back-Up and Disaster Recovery procedures, whilst having limited applicability (they are effectively work instructions to the IT team alone), demonstrate appropriate control over the issues described, and meet relevant audit trail requirements. In particular, the Disaster Recovery procedure has been written after an extensive (and successful) recovery exercise, undertaken in the last quarter of 2007/08, to 'prove' the model by which the Authority's systems and data could be recovered in the event of the destruction of the Authority's servers. This exercise was particularly useful in highlighting unanticipated problems between the theory of disaster recovery and its practical impact on the systems the authority currently operates, and the IT team now has a much fuller experience of the processes needed to deal with those problems, should actual disaster recovery become necessary.

RECOMMENDATION

7. That Members approve the ICT Policy and Procedures, as presented.

Steve Funnell
Senior IT Officer

Richard Burnett
Head of Finance & Resources

24 April 2008

Background documents: none

IT Policy and Procedures

Chief Executive Statement

It is the policy of the Yorkshire Dales National Park Authority (YDNPA) to respect all computer software copyrights and adhere to the Terms & Conditions of any licence to which the YDNPA is a party. YDNPA will not condone the use of any software that does not have a licence and any employee found to be using, or in possession of, unlicensed software may be the subject of disciplinary procedures.

It is the responsibility of all employees to read, fully understand and acknowledge their agreement to comply with the IT policies, and of their line managers to ensure that this is the case.

1. Software/Hardware Acquisition

All IT software and hardware (including devices that will interface with IT systems) must either be purchased by the IT Section or purchased after approval by the IT Section. This includes digital cameras, Personal Digital Assistants, laptops, mobile phones, printers, scanners and telephony devices.

Software and hardware must be purchased using the procedure laid down in the [Software Management Procedure](#).

2. Software Delivery

All newly acquired software will be delivered to the IT Section so that licences can be checked and Asset Registers updated. No other staff may take delivery of software.

3. Software Installation

Computer Software can only be installed on Authority machines under the direction of the IT Section.

Software installation will be carried out in accordance with the [Software Management Procedure](#).

4. Software Compliance and Documentation

All software documentation relating to proof of usage such as licenses and copies of invoices are to be kept in fireproof safes at either the Northern or Southern main offices. Original media for all software is to be kept secure at all times.

Documentation and security of media will be the responsibility of the IT Section as laid down in the [Software Management Procedure](#) and [IT Security Procedure](#).

5. Software/Hardware: movements

All software or hardware movements must involve the IT Section so that the appropriate software can be reconfigured as required and the asset register updated. This includes any re-organisation or if equipment is re-allocated.

6. Software/Hardware Disposal

The disposal or destruction of software, hardware and electronic data used by the Authority may only be carried out by the IT Section (for clarification, this excludes the deletion of e-mails and working files and updating the Intranet). The disposal will be in accordance with the procedure laid down in the [Software Management Procedure](#).

7. Prohibited Uses

Users are prohibited from:

- Installing shareware, freeware, abandonware, warez software, public domain software, privately owned software, evaluation, demonstration or training software, games, screensavers, fonts, unauthorised wallpaper other than that which is provided by the operating system. For further information, please see the [IT Security Policy](#).
- Unauthorised importing, retaining, printing, copying and transmitting of data or software that is protected by copyright laws. This includes trademarks, logos, words, letters, numerals or designs as described by the [Trade Marks Act 1994](#).

Where a valid business or training reason exists for the use of any software then staff are to follow the [Software Management Procedure](#).

8. Auditing

All users should be aware that the Authority electronically audits all computers to a regular schedule. Sample audits may also be carried out on a random basis.

All software is to be reconciled against the current licence library. The source of unauthorised software will be ascertained and disciplinary action may be taken as laid down in the Authority's [Disciplinary Rules and Procedures](#).

9. Laptops/Personal Digital Assistants/Mobile Devices

Only Authority-managed devices may be directly connected to the Authority's network. The Authority's IT policies apply to all Authority portable devices regardless of whether they are connected to the network or not. All such portable devices will have auditing software installed and checked in a similar manner to static systems.

Third party devices that require to be connected to the network are to be strictly controlled by the IT Section.

The procedure for the issue, configuration, use and security of portable devices is contained in the [IT Security Procedure](#).

10. Passwords

Access to Authority systems is controlled through passwords. The security and protection of individual passwords is the prime responsibility of the individual owner of the password.

Users must never document or divulge their password to another user.

Users are not permitted to use their passwords to allow other users or third parties to use a system.

Users should avoid the use of passwords that anyone can guess easily. Examples include the name of the employee or their relations, their telephone number, descriptions of their job or simple number sequences (such as 11111111 or 12345678).

Staff working away from their desk, even for short periods, should either log off or secure their workstation if they wish to remain logged on.

The password of anyone leaving the Authority will be cancelled once the IT Section has been informed of this departure by the line manager responsible for that post.

11. Viruses

Standard corporate anti-virus software will be deployed on all Authority devices that attach directly to the corporate network. Any exceptions to this rule must be authorised by the IT Security Officer.

The updating of virus software will be automatic where possible and configured by the IT Section. Users are not permitted to change configuration settings on anti-virus software or truncate update processes.

All media such as disc, CD ROMs, flashcards, memory sticks and other removable media must be scanned for viruses prior to being used on Authority systems.

In the event of discovering a virus the action to be taken is contained in the [IT Security Procedure](#).

12. Unauthorised Access/Hacking

Unauthorised access or hacking is an offence under the [Computer Misuse Act 1990](#). If any user believes they have access to unauthorised systems, software or data they should report the fact to the IT Department. If any user is aware of third parties gaining or attempting to gain access to unauthorised systems then they must report the fact to the IT Section immediately.

Any subsequent action regarding breaches of security should be taken in accordance with the [IT Security Procedure](#).

13. Data Protection

All processing of data relating to living individuals must adhere to the following Data Protection Act Principles:

- Personal data shall be processed fairly and lawfully
- Personal data shall be obtained only for one or more specified and lawful purposes

- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed
- Personal data shall be accurate and, where necessary, kept up to date
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes
- Personal data shall be processed in accordance with the rights of data subjects.
- 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.
- Personal data shall not be transferred to a country or territory outside the European Union 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.

Under no circumstances are employees allowed to take personal data off site or to load it onto portable machines or onto the drives of home computers, unless such data relates solely to the officer working off site (for example, their own appraisal records). Note that Citrix-enabled access for home working means that all such processing takes place on the Authority's servers.

Procedures for data protection are contained in the [Data Protection Policy](#).

14. Internet

The Internet as accessed through YDNPA systems is for Authority business. Personal or private business of a **transactional** nature may not be conducted using Authority systems. (Please see 'unacceptable use' section within Internet Acceptable Use policy, for clarification).

Users are not to visit websites of an offensive nature. Users are to follow the guidance in the YDNPA [Internet Acceptable Use Policy](#)

In certain circumstances there may be a business case for downloading software from the internet and if so then users must follow the procedure contained in the [Software Management Procedure](#) and after consultation with the IT Section. Otherwise, no software may be downloaded from the Internet. This includes pictures, films and music as well as software files for personal use.

15. Email

Users may not load or use any software received via email. Any officers receiving any files which are not standard business documents must inform the IT Section immediately.

In certain circumstances there may be a business case for receiving software via email and if so then users must follow the [Software Management Procedure](#).

Email is not to be used for confidential information without assuring additional safeguards (for clarification, this relates to any information that may have a value to a third party, for example bank details or payment transactions, where theft or other interference is a possibility). Generally email is not a secure means of communication.

Authority email systems are not to be used to send or knowingly receive offensive or illegal material and chain letters, or for conducting business other than that of the Authority. For clarification, this excludes occasional e-mails to friends and colleagues, provided these are not of a transactional nature and comply in all senses with the Email Procedures and Protocols; however, excessive use of the Authority's e-mail system for such purposes is unacceptable.

Email can be used as evidence in a court of law. The Authority reserves the right to access and disclose if necessary a users electronic and telephone communication.

Email is a formal means of communication. Employees must not make defamatory, racist or sexual remarks about any person or organisation. Nothing should be written on an email which would not be written in a traditional letter or memo. Offers and contracts made by email are considered as legally binding. All external YDNPA email will have the standard email disclaimer under each email.

Further guidance is contained in the [Email Procedures and Protocols](#).

16. Remote Access

The YDNPA ICT policies apply to all users who access the YDNPA network remotely regardless of which device or method is used, from when the network authentication is approved and remaining in force until the user logs off.

The IT Section under the direction of the Senior IT Officer will strictly control remote access to YDNPA systems for staff or any third parties. The procedure for gaining remote access is contained in the [Remote Access Procedure](#).

The procedure for offsite working using IT equipment is contained in the [Offsite Working Policy](#).

17. Back up & Maintenance

All YDNPA business data will be backed up daily. The IT Section is responsible for organising an adequate backup rotation and secure storage of media.

The procedure for data and software backup are contained in the [IT Backup and Disaster Recovery Procedure](#).

18. Disaster Recovery

The IT Section is responsible for ensuring that an appropriate business resumption risk assessment is carried out.

Details of the disaster recovery plan are contained in the [IT Backup and Disaster Recovery Procedure](#).

19. Disciplinary Procedures

YDNPA IT policies are implemented to safeguard the Authority from the various laws surrounding computer and software use. Any user found to be contravening these policies may be subject to disciplinary action in accordance with the Authority's [Disciplinary Rules and Procedures](#)

20. Policy Review

All of the YDNPA policies and procedures will be reviewed on a regular basis (at least every two years), in consultation with the IT Working Group, and any amendments or additions communicated to staff in an appropriate manner.

Information Security

Introduction

The purpose of this policy is to ensure that the Authority is adequately protected against threats to its security concerns. Breaches of security could produce consequences such as loss of reputation / business / assets (including data, equipment and money) / public confidence, credibility or goodwill, and could generate legal action.

The policy also aims to encourage in all employees and other users an awareness of the need for security and an understanding of their individual responsibilities.

1. Scope

The policy applies to all Members, Volunteers, partner organisations, external bodies and employees, including temporary staff and contractors, who may use the Authority's IT systems.

Risks for the Authority covered by this policy may relate to information held and processed by the Authority on behalf of clients or for internal purposes and to IT and other equipment.

2. Policy Statement

In order to achieve its objectives in a risk-free manner the Authority's organisation, procedures and technical activities must provide safeguards which ensure that the levels of confidentiality, integrity and continuity achieved are acceptable under all circumstances. The safeguards will seek to ensure that:

- (i) reasonable and cost effective measures are taken to protect the Authority's assets and operations from loss, damage or impairment;
- (ii) security risks are identified, evaluated, recorded and managed;
- (iii) vital and sensitive information is identified and protected from loss, unauthorised disclosure or modification;
- (iv) contingency plans for security emergencies are drawn up, kept under review and periodically tested;
- (v) actual or attempted security breaches are recorded, assessed and, where relevant, security measures are enhanced to prevent a re-occurrence.

3. Responsibilities

The successful implementation of the Authority's Information Security Policy cannot be achieved without the co-operation of all employees. It is imperative, therefore, that all are aware have, and fully comply with, the security requirements of their office and function.

It is the responsibility of all line managers to ensure that staff fully comply with the relevant security procedures.

Specific security duties have been delegated as follows:

| | |
|--------------------------|--|
| Senior IT Officer | |
| 1 | Ensure that appropriate arrangements exist for the implementation of the Information |

| | |
|----|---|
| | Security Policy. |
| 2 | Report to the IT Working Group on security related matters. |
| 3 | Review the Information Security Policy and procedures as necessary. |
| 4 | Advise the IT Working Group on necessary enhancements or changes to the Information Security Policy. |
| 5 | Perform security reviews in accordance with a previously agreed plan, and where necessary, ad hoc inspections. |
| 6 | Advise on, and agree with the IT Working Group, the security aspects of projects under development. |
| 7 | Provide specialist advice on all aspects of security, including: <ul style="list-style-type: none"> • telecommunications security; • the security aspects of current legislation. |
| 8 | Commission reviews of specific areas of security concern. |
| 9 | In co-operation with the IT Working Group install a method of monitoring security-related activities in the Authority's Local Area Networks, Wide Area Network and Server installations. |
| 10 | Investigate reported breaches of security, and record the results of such investigations. |
| 11 | Promote security awareness within the Authority. |
| 12 | Review the security arrangements of suppliers to the Authority of IT and related services. |

| | |
|----------------------|--|
| Line Managers | |
| 1. | Ensure compliance with procedures. |
| 2. | Promote and champion security awareness. |
| 3. | Inform the Senior IT Officer of any serious breaches of security which may occur in their areas of responsibility. |

4. Security strategies and measures

(i) IT Equipment. All equipment and consumables must be subject to appropriate access controls and procedures must exist, and be complied with; to ensure they cannot be stolen, destroyed or misused.

(ii) Contingency Planning/Disaster Recovery. Contingency plans should exist to enable the Authority's systems to resume operation in a timely manner following serious disruption to those systems' availability. These plans will be continually reviewed and updated as new systems or facilities are developed.

Copies of all data will be taken at regular intervals, and stored in a protected environment, away from the immediate site at which the data is normally used. Further copies of sensitive or valuable data will be kept and stored at alternative premises. Retention times of all backed-up data will be sufficient to comply with business and legal requirements.

Alternative methods for processing critical systems will be reviewed and tested regularly.

(iii) Logical Access. Where access is required to a computer system, permission must be sought from the person performing the appropriate security administration function. If access is required to data which has not been previously authorised permission must be obtained from the data owner.

Networks may only be directly connected to the Internet through a Firewall which has been approved by the IT Working Group and the Senior IT Officer.

Those employees who are entrusted with a log-on code and password will be accountable for all activity against that code. It is therefore necessary to maintain passwords in a secure manner.

(iv) Systems Development. New IT systems must demonstrate appropriate security features before installation commences. The Senior IT Officer will monitor the development and implementation of systems and facilities which they consider to be particularly sensitive.

(v) Data Communications. Where sensitive data is transmitted through internal or external telecommunications networks, the Authority's security procedures will guard against unauthorised access to that data.

(vi) Use of Hardware and Software. Policies relating to the use of personal computers include the following: the loading of unauthorised software and data is strictly prohibited; computing equipment, software and data used on YDNPA premises and elsewhere must be adequately protected; the acquisition and use of PC hardware and software must be properly authorised and controlled.

(vii) Disposal of Data and Media. Information that is no longer needed but is still sensitive will be destroyed in a secure manner. Waste materials (such as used paper, carbon paper, printer ribbons, magnetic tapes, diskettes and CDs) which contain sensitive information must be destroyed as soon as practicable.

(viii) Incident Reporting. Any security breach will be reported to the IT Officers who will advise on any further action.

5. Network Security

The Authority's objective is to provide staff with access to all the computer facilities they need from a single PC. Staff will use this computer to communicate and share data with other users, whether local or remote, via their office Local Area Network (LAN).

The network provides staff with access to shared data, common points of access to internal and external systems and access to shared printers.

All reasonable precautions must be taken to ensure that data is secure at all stages in the network. Our security procedures must ensure that our computer systems are secure and data is adequately protected.

The following procedures apply to all links to office networks, whether implemented by the Authority, a client or any other party.

A **Firewall** must be installed between any YDNPA LAN and each remote link to ensure only authorised traffic can be transmitted. The Firewall must be configured defensively to allow only authorised network traffic to pass. Where a bridge or router is installed at the remote end of the link, complementary or identical Firewall controls should be applied.

All proposals to install **new connections** to the network must be reviewed and approved before installation. Approval must be granted by the Senior IT Officer. The proposal must identify any change that may increase or create any security exposure.

Where an external site is new to the Authority, all external links must be reviewed to confirm that the impact of the new connection will not impair their security. Any changes resulting from the review must be implemented before the new network can be approved.

The Firewall platform must be held in a secure room with access restricted to a limited number of authorised personnel.

6. Prohibited Uses

Prohibited uses of the Authority's communication systems include, but are not limited to:

- importing, retaining or communicating data (documents, software, information, images or other materials) that is unauthorised or unlawful or in violation of Authority policy, including (but not limited to) data that is (or could reasonably be considered to be) defamatory, obscene, or potentially offensive to any other party, whether the other party is an employee, a client or other person or group of people or organisation;
- copying or transmitting data protected by the copyright and related laws, without copyright or similar authorisation;

- the unauthorised use of passwords to gain access to another user's information or communications;
- electronic "snooping", which includes but is not limited to "hacking" into the voicemail, electronic mail or other data addressed to others within the Authority communication systems;
- sending, forwarding, redistributing or replying to "chain letters;"
- knowingly introducing a computer virus into the Authority communication systems and any other non-compliance with the Authority's rules and guidelines concerning the avoidance of computer viruses;
- using any such systems to solicit or conduct business other than the business of the Authority;
- soliciting or advocating for issues, causes or organisations of any kind when such solicitation or advocacy is deemed by the Authority to be personal in nature and/or not recognised as clearly furthering the reputation and interest of the Authority;
- unauthorised fundraising of any kind;
- introduction of unlicensed products;
- import, transmission or playing of computer games;
- personal use of systems which is habitual or frequent.
- The above-prohibited uses include the use of unauthorised "screensavers" or "wallpaper".

For the avoidance of doubt, the location of a prohibited item or items in a personal or password protected part of Authority communications systems (whether stored on a Network drive or hard drive or elsewhere) does not exclude an individual from the above prohibitions.

Employees who are in unsolicited receipt of communications which may breach the prohibited uses above, may forward them to the Head of Finance and Resources and/or the Senior IT Officer, without that particular action itself constituting an offence under this policy. The said officers will pursue such matters with those responsible for the initial transmission.

The Authority will cooperate fully with any police inquiry or other lawful inquiry into any alleged illegality arising as a result of prohibited use, recognising that this may assist in the criminal prosecution of staff involved.

7. Access and Disclosure

The Authority reserves the right to access and disclose the contents of a user's electronic and telephonic communications at any time, but intends to do so only when it considers it has a business reason. Determining when such a business reason exists shall be within the Authority's sole and absolute discretion. Business reasons to access and disclose these communications may include, but are not limited to, the need to solve technical problems, the investigation of allegations of theft or other crime, the prevention of unauthorised disclosure of confidential or proprietary information, suspicion of personal abuse of Authority communication systems, conducting an investigation under any Authority procedure (for example, disciplinary, capability or grievance), the need to create space on or re-order the contents or methodologies of the Authority's IT network and general review of communications. The Authority may use information regarding the number, frequency, sender, recipient, content and address of any communications for any business reason.

8. Permitted personal use

The Authority recognises that many employees would wish to use the Authority Communication Systems for support in their studies for professional and other examinations and this is permitted.

Incidental and occasional personal use for other reasons (and this extends to the use of telephones for emergency personal use) is also permitted provided it does not contravene any of the prohibited uses detailed above, and is not habitual or frequent in nature. Such use must only be undertaken outside working hours (which definition includes lunch breaks).

Staff should confirm in advance with a Departmental Head the permissibility of any personal use, which may not fall within the definition of permitted personal use.

Software Management Procedure

Introduction

The Purposes of this procedure are to:

- ensure that the Authority maintains compliance with the legal requirements for using commercial and other software on its ICT equipment;
- assist in maintaining a comprehensive database of software licenses owned and used within the Authority;
- ensure that software purchased by the Authority is compatible with hardware and operating systems in place.

1. Definitions

Software is typically divided into two categories.

- Operating system software that is designed to handle tasks specific to the management and interaction of the hardware and software components of a system. Examples of operating system software include Windows XP, Windows Server 2003, and Citrix Metaframe. Anti-virus and other security applications are included under this heading
- Application software that is designed to help users solve problems and improve productivity in their work activities. Examples of application software include Word, Excel, Access, Powerpoint, Mapinfo, and SunSystems.

The following text refers to the purchasing of software in all cases. In respect of licensing it is to be taken as read that this policy also refers to the acquisition, installation and use of any non-chargeable applications; in all cases such software will also be subject to licensing terms and conditions that must be adhered to.

2. Software (and Hardware) Purchase Requests

The IT Section must be informed of all software purchase requests before orders are placed so they can ensure software purchased is compatible with Authority systems, that it does not duplicate functionality in software already purchased and made available, that support and maintenance issues have been properly addressed and that it is being purchased on the most advantageous terms to the Authority and in line with Financial Regulations. Please note that this approach applies equally to Hardware purchases; all Hardware will be ordered by the IT Section.

3. Server Operating Software, Workstation Operating Software and Anti-virus software

Purchase, installation, upgrading, support and maintenance of server operating software (including backup software), workstation operating systems and anti-virus software is the responsibility of the IT Section. The Senior IT Officer is responsible for ensuring that all such software is purchased and operated in accordance with Authority Financial Regulations and the terms and conditions of the respective licenses. Any such purchases will normally be funded from central IT budgets. In circumstances such as the purchase of a major new corporate application requiring additional server hardware funding may be required from other Departments within the Authority.

4. End User Applications

Each member of staff will have access to a Microsoft Office Professional licence. This includes Word, Excel, Access Outlook and Powerpoint. Other software licences for use with GIS (Mapinfo) and the finance system (SunSystems) will be provided on a 'needs' basis.

Any requests for new software will be considered by the IT Working Group.

5. Installation and Registration of Software

Authority computers must be kept both software-legal and virus free.

Each software package being used on an Authority computer must be properly purchased, licensed and registered. Software must be registered in the name of the Authority or the department or section where it will be used. Software must not be registered in the name of an individual staff member.

Where users are required by their work to download software from the intranet (and for software received via e-mail), they should first consult with, and gain approval from, the IT section before installation.

6. Software Inventory

The IT Section will create and maintain a software register of all software licensed for use at each site. This register will be used to audit and compare the authorized software list with software actually loaded on each computer.

7. Disposal

Any software that is identified as no longer required will be deleted from all users' systems by the IT Section and any installation media (such as compact discs) will be destroyed; the license owner will be informed that the Authority is no longer using that application. All disposals will be in line with Financial Regulations.

Internet Acceptable Use Policy

Introduction

This Acceptable Use Policy applies to all persons granted access through any YDNPA IT resources and equipment, regardless of location. This includes staff (including temporary staff), visitors, contractors, students, members and volunteers. For the purposes of this document the 'Internet' is any facility accessed electronically via the Authority's Internet Service Provider (ISP).

1. Disclosure

The Authority accepts that the use of the Internet is an extremely valuable business, research and learning tool. However, users should be aware that misuse of such a facility can have a detrimental effect on other users and potentially on the Authority's public profile. As a result, the Authority will monitor:

- The volume of internet and network traffic
- The internet sites visited

The specific content of any transactions undertaken using the internet will not be monitored unless there is a suspicion of unacceptable use.

The Senior IT Officer will maintain web filter software to minimise the risk of officers inadvertently accessing unsuitable or malicious web-based material, including sites that may cause data corruption or spread viruses. Where this software blocks access to a legitimate website, approval to unblock that site should be sought from the IT Section.

2. General principles

- Use of the Internet by staff is permitted and encouraged where such use supports the goals and objectives of the Authority.
- Use of the Internet is monitored for security and network management reasons. Users may also be subject to limitations on their use of such resources.
- The distribution of any information through the Authority's network is subject to the scrutiny of the Authority. The Authority reserves the right to determine the suitability of this information.
- The use of computing resources is subject to UK law and any illegal use will be dealt with appropriately. For example the Police are entitled to right of access to recorded data in pursuit of a crime.
- Access to some sites is blocked by the Authority's security systems, a process that seeks to manage out the risk from sites which may have a virus or other operating risk associated with them. Where such access is needed for business reasons, the IT team should be contacted to permit access to that site.

3. Unacceptable use or Behaviour

During working time, officers must not use the internet for any purpose other than in connection with their duties, and at any time (whether working time or not) officers must not:

- Visit Internet sites that contain obscene, hateful or objectionable materials.
- Visit sites that promote racism, drug or substance abuse.
- Visit sites that contain pornographic material.
- Visit sites that are illegal or promote illegal activities or violence.
- Use chat rooms or other forms of 'social networking' (including Facebook, Myspace, Second Life or blogging) other than e-mail. Where a genuine business case can be made, use may be permitted subject to any likely impact on other users.
- Use the Internet for personal financial gain of any type.
- Use the Internet for online gambling or gaming of any nature.
- Use the Internet for shopping or online banking, or any other transactions not related to the work of YDNPA.
- Make or post indecent remarks, proposals or materials on the Internet including racist or sexist jokes and defamatory comments.
- Upload, download or otherwise transmit commercial software or any copyrighted materials belonging to parties outside of the Authority, unless this download is covered or permitted under a commercial agreement or other such licence. This includes but is not exclusive to: Images, music, video, applications, drivers, screensavers and utilities.
- Download any electronic files other than documents used for official YDNPA business.
- Intentionally interfere with the normal operation of the network, including the propagation of computer viruses and sustained high volume network traffic that substantially hinders others in their use of the network.
- Monitor Network Traffic Content with scanning or sniffer software.
- Access or enter into peer to peer file sharing or attempt to download any software that allows this practise.
- Use the YDNPA internet connection to access personal web mail.
- To use the YDNPA internet connection to access or configure Instant Messaging Services.

Officers whose use of the internet is identified as unacceptable will be subject to the Authority's [Disciplinary Procedure](#).

The Authority will permit use of the internet within an officer's own time (for example, when 'clocked out' during a lunch-break), subject to the above conditions: such use is therefore restricted to viewing websites. Please note, however, that if such use is considerable, and to the extent that it materially reduces the speed of the Authority's internet connection, then this general permission may be withdrawn. Where it is identified that officers are accessing websites that do not relate to the Authority's work, either during work time and/or to an inappropriate degree, then this will be an issue for their line manager to resolve and does not form part of this policy.

4. Users should:

- Report immediately to the Senior IT Officer if you become aware that there has been unauthorised access to your computer.
- Record any instances where you have accessed inappropriate sites by accident. For example this may be through mistyping an address or spam email link.
- Log out of the computer when you have finished.

Remote Access Procedure

Introduction

The YDNPA network will use remote connection technologies to connect resources to people both locally, over the WAN and also over the Internet. This will make the Authority more effective but also brings a greater risk to the network. The aim of this procedure is to reduce the risk to the security of the network whilst utilising the benefits of remote access.

1. YDNPA/Private Equipment

- Unless explicitly agreed with IT Officers, only YDNPA equipment may be connected directly to the YDNPA network at YDNPA sites.
- Portable YDNPA devices may be connected to the network via the Internet at any location using the account details provided by the IT Section.
- Privately owned or third party equipment may be connected to the network via the Internet only.

2. Citrix Environment

- If users require access to their Citrix Desktop from a remote location they are to seek authorisation from their line manager and ensure they are conversant with the [Offsite Working Policy](#). If authorised, the IT section are to check the availability of licences and configure Citrix Secure Gateway to allow the user to connect.
- Users are to connect to the network via the Internet using a web browser and a URL address specified by the IT Section. The address will connect the user to the Citrix Web Access site. It will be the responsibility of the user to download the small Citrix client file from this site to the users' local device to enable remote access. The responsibility for the users' local device including software is solely with the user and the Authority accepts no liability for private equipment used for this purpose.
- Once connected to the desktop only the authorised user may use the session. It is strictly forbidden for anyone else, including family members or other third parties, to use the remote connection. When the session is complete the user is to log off immediately and not leave the session open. Failure to comply with this directive exposes the Authority's systems to significant risk and may result in the withdrawal of this facility and disciplinary action where appropriate.

3. Authentication & Access

- All users remotely accessing the network for Citrix sessions or to remotely view email will be required to use their username and password. Where possible the IT Section will enable traffic travelling over the internet to be automatically encrypted.
- Unauthorised attempts to access the network will be monitored by the IT Section and brought to the attention of the IT Security Officer.
- Access to folders of particular importance or of a critical nature will be restricted to those who require access as part of their job function. Critical folders will be audited for attempted access violations.

4. Third Party

If any third party organisations require remote access to the YDNPA network for maintenance or support work then a request should be made to the IT Security Officer.

Staff must not agree to support contracts of this nature unless they have first consulted the IT Security Officer. The IT Security Officer will liaise directly with the third party/vendor to verify the conditions of the connection. If necessary an account should be created within Active Directory and restrictions applied to the account. The account is to be disabled when not in immediate use.

5. Remote Control Software

Users must not install any remote control software on YDNPA equipment. If software of this nature is required then a request must be made to the IT Security Officer together with the business case for the installation. The IT Section personnel are the only staff permitted to install and monitor this type of connection.

6. Citrix Shadowing

It is possible in the Citrix environment for a user session to be shadowed remotely by IT Support officers. This can be useful when a user is having problems or is experiencing errors, which a support officer can help to solve directly by joining that session. The privacy of the individual will always be respected so IT Section will configure the IT network so that a request has to be issued and accepted by the user before allowing remote support.

Email Procedures and Protocols

Introduction

Email is a quick, useful method of communication. However, when corresponding via e-mail it is necessary to balance this speed of communication with good practice, common sense and professionalism. The following procedures aim to achieve this and should be applied in all email correspondence in order to ensure a safe, secure, stable, email environment.

1. Disclosure

- The Authority reserves the right to monitor usage.
- In general, access to read the **mailbox** or mailbox archives of other users will only be granted to staff responsible for investigating system failure or system misuse and then only to look at information as necessary to repair or protect the systems or to investigate use that may be illegal or in contravention of the IT Policy. Access to read officer's mail by job share partners, administrative support officers or colleagues during periods of leave will only be granted on the written (or e-mailed) confirmation by the owner of that e-mail account that this is acceptable.
- Access to a user's **personal documents** stored on the users personal drive, My Site private area or in their email mailbox will only be granted to another user if a written request is received and authorised by the Head of Department of the user concerned.
- Email or voicemail messages, however confidential or damaging, may have to be disclosed in court proceedings, during internal or criminal investigations if relevant to the subject of such proceedings or investigations. Similarly, public disclosure of emails may be required under the Freedom of Information Act.

2. Email Addresses

- All staff will be allocated an email address in the naming convention:
firstname.surname@yorkshiredales.org.uk
- If a new member of staff requires an email address on their first day of work, the relevant line manager should contact the IT section well in advance with the details of the new employee.
- Email addresses are for use in Authority business and may not in any circumstances be used for private business (transactional) use.
- Requests for generic email addresses should be made to the IT Section with intended purpose and proposed name. Naming and management of the generic mailbox will be agreed between the requesting party and the IT Section.
- Requests for email addresses or accounts that are not suffixed yorkshiredales.org.uk should be made to the IT Section who will acquire and arrange management of the address or account.

3. Email Data Management

- Users on the network are not to use the inbox or Microsoft Outlook folders as a storage system. Excessively large mailboxes can be detrimental to the performance of the email

system and is an inefficient, insecure method of storing data. A storage quota limit will be applied to all mailboxes to ensure maximum availability of the email system. A warning message will be sent when a mailbox storage limit is about to be reached.

- All unwanted messages should be deleted as soon as possible from the system. This includes items in the 'Sent Items' and 'Deleted Items' folders.
- If an attachment or e-mail is likely to be needed for future reference it should be saved to the correct location on the network, where it can be made available to all potentially interested parties. If the body of text in an email is needed it can either be saved as a message or the text can be pasted into a Word document.
- The maintenance of mailbox accounts will be the responsibility of the IT Section and will include the deletion of mailboxes if authorised by the relevant Head of Department.

4. Email Good Practice

4.1 General

- Offers and Contracts made by email are legally binding; take care not to inadvertently commit the Authority to any particular course of action. Legal advice must be sought before entering into any email communication of this nature.
- Users are not to send, forward or retain material that is subject to copyright, patent or trademark protection.
- Users should not be overly reliant on email as their only communication tool. Verbal conversation remains the most appropriate form of communication in many situations.

4.2 Receiving Email

- If an attachment is not a standard business document the recipient must inform the IT Section. Users must not install software received by email.
- If a user is not sure what an attachment is for, or why someone has sent it, they must not open the attachment.
- Email should be checked during the working day and dealt with in a timely manner.
- If users receive a "chain letter" they must not reply to it or forward it on to others.
- If users receive email which is or suspected of being of an illegal nature then it should be reported to the appropriate line manager.

4.3 Sending Email

- Ensure that the message makes it clear why you are sending the e-mail, and identifies the deadline for any action or response.
- Keep text in the font 'Arial', and use only plain backgrounds.
- Email should not to be used for confidential information without assuring additional safeguards (for clarification, this relates to any information, for example, that may have a value to a third party, such as bank details or payment transactions, where theft or other interference is a possibility). Generally email is not a secure means of communication, and always offers opportunities for hackers.
- Defamatory remarks should not be made. Do not make racist or sexual remarks or use language that could be construed as bullying/harassment about any person or organisation.
- Do not send or forward email to any large group unless there is a genuine reason for them to read it. Consider using other means, such as the intranet, to advertise information to all staff.

- Avoid using attachments for internal email wherever possible. Consider leaving the document on the network and use a hyperlink in the email text. If attachments are sent, identify in the e-mail what you are expecting of the recipient, and - if appropriate - which parts of the attachment are relevant.
- Use meaningful text in the subject field: do not leave the title blank.
- When sending email to external addresses, consider the possibility that this action may inadvertently reveal email addresses to third parties. When sending to a list of external email addresses, consider sending using the "BCC" field rather than the "TO" field.
- Do not circulate warnings about any virus risk, but consult the IT Section. Many virus warnings are hoaxes. The IT Section can analyse them and take any steps needed to protect the Authority.
- Check your reply settings - it is easy to use "Reply-All" by mistake, and this could be embarrassing for you and annoying to others.
- Use a signature at the end of your e-mail: your name, job title and e-mail address or telephone number.
- Do not send non-specific email such as the weather or advertisements and consider using other media such as the intranet for giving out generic information.
- Finally, if you would not write something in a letter or a memo, then don't send it in an e-mail either.

4.4 Disclaimer

To help protect staff and the Authority all YDNPA email will automatically have the following standard email disclaimer at the foot of each email:

“Warning

This email and any attachments may contain information that is privileged, confidential or otherwise protected from disclosure. They are intended solely for the named recipient(s), and must not be used by, or copied or disclosed to, any other persons. If you are not an intended recipient please accept our apologies, contact us to let us know the email has gone astray, and then delete it. Unauthorised copying, distribution or disclosure is prohibited and may be unlawful. Unless otherwise indicated, copyright in the email and all attachments belong to the Yorkshire Dales National Park Authority. Although this email and any attachments are believed to be free of any virus or other defects that might affect any computer or IT system into which they are received, no responsibility is accepted by the sender for any loss or damage arising out of any malicious software, virus or other defect.”

Backup Procedure

Introduction

This procedure describes the process to be followed by IT Officers in preparing back-ups of the Authority's IT systems and data.

1. Software

YDNPA uses Symantec Backup Exec Software to secure data and applications to tape. Agents are used to backup remote servers, SQL databases, Exchange mailboxes and Sharepoint.

Backup Exec software is installed on the finance1 and sqlshare DL 380 servers and these are connected via SCSI cables to the external tape drives.

2. Hardware

Two HP Storage Works SSL 1016 tape autoloaders backup up to 400Gb Ultrium tape media. These devices have 16 slot tape carousels and 1 tape drive each.

3. Backup Schedule

Full Backups

Full data backups are carried out on Tuesday, Friday and the last day of the month. When the last day of the month is a Tuesday or Friday then only the monthly backup is carried out

Differential Backups

Differential backups are carried out on Sunday, Monday, Wednesday, Thursday and Saturday. When the last day of the month is one of these days then only the monthly backup is carried out

System State and Active Directory Full Backups

This is run every Thursday from the Backup Exec installation on the Finance1 server

4. Backup Selections

The following schedule lists the data files that are backed up on each server.

Finance1 Server

Finance1 server selections

C:Drive

E:Drive

Users

SQL Server

SunSystems

TrueTime

Backup Exec DB

System State

Citrix4 server selections
C:Drive
System State

DC1 server selections
C:Drive
System State

Sharepoint server selections
C:Drive
Sharepoint Resources
System State

Isa1 server selections
C:Drive
System State

YDNPADData server selections
C:Drive
E:Drive
 Mapdata
 Planning
System State

SQLShare Server

Sqlshare server selections
C:Drive
D: Drive
 Data
 Profiles
SQLServer
 Citrix Data
 Sharepoint Data
 Backup Exec
System State

Citrix5 server selections
C:Drive
System State

Citrix6 server selections
C:Drive
System State

DC2 server selections
C:Drive
System State

Exchange
C:Drive
Exchange Mailboxes
Exchange Public Folders
Information Store

5. Offsite Storage and Retention Periods

Full backups carried out on a Friday and the last day of each month are to be stored offsite in the fire safe located at the Retail Services warehouse, Cragg Hill Road, Horton in Ribblesdale.

Friday full backups are overwrite protected for 4 weeks. After this time they are available to be re-used as backup media.

Month end full backups have an infinite overwrite protection and must be kept for a minimum period of 5 years

All tapes must be labelled with the server name finance1 or sqlshare, the tape name e.g. LTO123456, the backup date and tape sequence number.

Disaster Recovery Procedure

Introduction

In the event of a major incident affecting the Authority's ICT infrastructure there would be severe consequences. Many services would quickly be brought to a standstill in the event of prolonged computer breakdown. The vulnerability of the Authority's services to the effects of a computer failure have increased markedly in recent years as more and more reliance has been placed on computer computerised system to manage services. The current drive for eGovernance will further increase this reliance in the future.

1. Definition of Disaster

“For the purposes of this plan a Disaster is defined as loss or damage of part or all of the Authority's ICT Infrastructure, which would have a high, or very high, business impact on the Authority.”

Disaster, as outlined in the above definition, includes :

- a) Total loss of Yoredale
- b) Loss or technical failure of one or more network servers
- c) Loss or technical failure of network infrastructure such as hubs/switches/routers/communications links
- d) Loss or failure of the Wide Area Network
- e) Loss or technical failure of the telephone system
- f) Extended loss of electrical power
- f) Failure of a key software system

Key software systems include :

- i) Sun Systems – Financial System
- ii) Exchange Server 2003 – the Email System
- iii) PACS – Planning Application Control System
- iv) HBSMR – Historic Buildings and Sites and Monuments Record
- v) Mapping systems for Rights of Way management

2. How the procedure is activated

In the event that a disaster is identified by the Senior Management Team (or by the Senior IT Officer), the Senior IT Officer will be responsible for activating the procedure and monitoring the progress of disaster recovery, reporting to senior management and undertaking any further action as necessary.

3. Overview of ICT Infrastructure

Wide Area Network

The YDNPA premises at Colvend Grassington, Yoredale Bainbridge, Aysgarth Falls TIC, Dales Countryside Museum and TIC Hawes, Malham TIC, Stonedykes barn Workshop Settle and the

Retail Services Warehouse Horton-in-Ribblesdale are all connected by a Wide Area Network. This network is provided under contract by North Yorkshire County Council. The service is provided by a combination of wireless and kilostream links.

Sites

Yoredale

This is the main site housing the YDNPA ICT infrastructure. There are 14 file servers providing the applications and data storage resources to users at all connected sites. Yoredale also contains one of the main telephone switches together with network communication switches, routers and firewalls.

The server room at Yoredale is located on the first floor and has no external access. Equipment is protected from variation in the utility electricity supply by uninterruptible power supplies (UPS). These also provide a backup power supply should the utility supply fail completely, allowing equipment to be shut down in a controlled way. The server room also houses an air conditioning unit to maintain equipment at a suitable operating temperature.

Colvend

Houses second main telephone switch, communication switches and router.
Some local processing on workstations

The equipment room at Colvend is located on the first floor and has no external access. Equipment is protected from variation in the utility electricity supply by an uninterruptible power supply. This also provides a backup power supply should the utility supply fail completely, allowing equipment to be shut down in a controlled way

Aysgarth Falls TIC

Telephone switch, communication switches and router.

Dales Countryside Museum

Telephone switch, communication switches and router.

Grassington TIC

In ICT terms this is part of the Colvend Local Area Network

Malham TIC

Communication switches and router

Horton Retail Services Warehouse

Communication switches and router

Stonedynes Workshop

Telephone switch, communication switches and router

Reeth TIC & Sedbergh Ranger Office

In ICT terms these are not part of the YDNPA WAN and are not considered in this document.

4. Risk Assessment and Business Impact Review

Wide Area Network

There are a number of potential points of failure of the Wide Area Network (WAN). Loss of service at any of these points would have varying effects on the organisation.

The responsibility to fix these faults lies with NYCC and the network supplier MLL Communications.

Sites

Yoredale

In the event of a major loss of IT equipment and networking at the Yoredale offices the following steps would be taken.

Determine whether Yoredale could still be used as offices, if not relocate systems to alternative YDNPA premises that had WAN connection, e.g. Hawes Museum or Colvend.

Ascertain whether any equipment could be salvaged; if 'yes', later steps should be taken for using this salvaged equipment wherever possible.

Initial replacement servers would be hired in. This would be the quickest means of obtaining equipment of the required configuration. Turnaround time for this is typically 24 – 48 hours

A core number workstations would be replaced by purchase of thin client machines as these are very quick to deploy (10 - 15 minutes to unpack connect and configure).

Systems would be rebuilt in the following order:

- Domain Controller DC1 to re-create domain and user information.
- Data server YDNPADATA (this would provide the source server for restoring all other applications and data)
- Application and Data server SQLSHARE required for Citrix restore
- Citrix server Citrix4 to recreate all application software
- Citrix Secure Gateway to provide remote access

At this point the PACS and HBSMR applications would be available. The following servers could then be rebuilt in parallel:

- Finance1 to restore the SunSystems finance application
- Exchange to recover email services
- Citrix5 & Citrix6 to provide additional connectivity

The second domain controller DC2 to provide login resilience. At this point all core systems referred to in "Key Software systems" above would be available. The following servers would then be rebuilt:

- Sharepoint to restore intranet
- Isa1 to restore internet access management

At this point all YDNPA systems would be restored

Other Locations

In the event of the loss of the following premises staff would be relocated or would work from home

- Colvend
- Aysgarth Falls TIC
- Dales Countryside Museum
- Grassington TIC
- Malham TIC

Reeth TIC
Sedbergh Ranger Office
Horton Retail Services Warehouse
Stonedynes Workshop

5. Disaster Recovery Plan Testing

A full test of the disaster recovery process was carried out in February 2008 using hired equipment. All core systems were successfully restored; in addition all non-critical systems and data were restored and tested.