- B.10 Managing HER information systems
- B.10.1 Technical support for HER systems
- B.10.2 Data security
- Access and modification control
- Viruses
- Remote Trojan Horse attacks, Worms, Hoaxes
- Backing-up data
- B.10.3 Procuring new information systems
- HER databases
- GIS software
- Contracts
- B.10.4 Data migration

B.10 Managing HER information systems#

B.10.1 Technical support for HER systems#

HER computer systems may be based on a corporate network or on stand-alone PCs and may make use of standard commercial packages or bespoke systems. However installed, computer systems need technical support for both hardware and software. Such support may be available from corporate IT departments but, even where centrally provided, the actual support may be supplied by contractors. HER managers are recommended to consider carefully the level of support that they require to keep systems running and where possible reach appropriate 'service-level agreements'. These agreements might cover:

- support from hardware engineers to maintain and repair computer equipment
- provision of replacement hardware if repairs are undertaken offsite
- support from software developers to maintain or develop databases
- support to maintain or develop GIS
- provision of a telephone help desk to answer enquiries about using databases or GIS.

B.10.2 Data security#

All aspects of a computing system can affect data security. Hardware components can fail or become damaged. Software problems can lead to the corruption of data. Security can be compromised through unauthorised access and modification of data or through loss of confidentiality. Computer systems and the data they hold need to be protected and to have tried and tested recovery procedures in place. It is expected that HERs run by a local authority will have adequate security, including firewalls and anti-virus protection. The need for this needs to be emphasised for HERs provided by Trusts.

Access and modification control#

Some form of access and modification control is necessary to secure HER systems. The HER officer plays a crucial role in deciding levels of access and security for both staff and other users. Passwords are usually seen as a suitable way of guarding against unauthorised access to a computer system but may not provide the level of security that is anticipated.

One problem is that users tend to choose passwords that are easy to remember, which unfortunately are therefore also easily discovered by 'hackers' (people who gain unauthorised access to computer systems). Ideally passwords should be at least eight characters long and be a mixture of numbers

and letters in upper and lower case, for example eLc1ddZ. They should not be based on easily obtainable information such as names or telephone numbers. Security is improved if the system restricts the number of chances a user has to log on. Most modern operating systems provide for password encryption.

Passwords can also be required at different levels of the system, such as network login, user account, specific machines and application, and even on specific directories and files. The kind of access users are allowed can often be controlled as well, for example files and directories set to 'read only' in order to prevent unauthorised modification. The usability of the system needs to be considered before implementing passwords at too many different levels, as overuse can cause its own problems.

Viruses#

A computer virus is a self-replicating computer program that may or may not be harmful. Some viruses simply display a message on screen while others destroy data stored on the system's hard disk. Viruses are the scourge of contemporary computing and they are extremely prevalent. Figures from MessageLabs, a leader in the provision of secure content management services and anti virus services, over 10 percent of emails contain a virus. In 2000 McAfee, an anti-virus software producer, estimated that over 45,000 types of virus were known. Today the figure is well over 70,000. A 'Trojan horse' is another type of program, usually grouped with viruses, which is introduced on to a computer system and triggered by pre-defined actions. Trojan horses are not self-replicating but they are invariably destructive.

It is essential that any computing system is protected by anti-virus software. This software must be regularly updated to combat new viruses as they are discovered. There are numerous software packages available and, if a system is not already protected, HER managers should make it a priority to install one of these.

All files should be scanned by the virus checker before being loaded into a system.

Remote Trojan Horse attacks, Worms, Hoaxes#

Most organisations will have a firewall in place as part of their IT strategy, however, individual machines increasingly need the protection of personal firewalls. Hackers can compromise poorly secured web sites with malicious code which exploits browser vulnerabilities to upload and execute a remote access Trojan Horse on the browser host machine, hence the possibility of bypassing an organisational firewall. Browser patches for vulnerabilities and firewall settings necessarily must be kept up to date.

Useful websites:

CNET News http://news.cnet.com/

McAfee (virus protection software) http://www.mcafee.com/uk/

Symantec (secure content management services) http://www.symanteccloud.com/en/gb/

Symantec ('Antivirus Research Centre') http://www.symantec.com/avcenter/index.html

Backing-up data#

No matter what precautions are taken, data is probably going to be lost at some time either accidentally or through malice or theft. There is a need for a strategy to be in place which covers both the backing-up of data and a tried and tested recovery plan. Some form of risk assessment should be undertaken.

HERs held by local authorities will usually be part of that authority?s back-up routine, which may mean a twice daily back-up and set procedures in place for restoring files which have been lost or corrupted. These systems may be held off site, in RAID disk arrays, where data is mirrored on more than one disk, or Storage Area Networks (SANs), which allow the sharing of back-up equipment between computers.

Stand-alone HERs will need their own back-up procedure. A traditional one is GFS (grandfather, father, son), where daily back-ups are sons, weekly back-ups are fathers, and monthly back-ups are grandfathers, each level able to be overwritten after a suitable interval, except for the grandfather, which is kept. High capacity DVDs and memory sticks are suitable mediums for this sort of back-up, with the advantage that they can be kept off-site for added security. Using GFS may be excessive for many situations, especially if data remains static for long periods, but it can be adjusted so the interval are longer or whenever data is updated. There are also now online back-up services, which may also be an option for some HERs.

If the HER is remotely hosted, the HER Officer should ensure that the host has adequate back up facilities in place. It is good practice to attempt a test restore on a separate PC or server to ensure back up procedures are adequate. This should be repeated after upgrades and alterations to the system. Backup and restore procedures should be included in disaster recovery plans. If complete disaster happens and your back-up strategy fails or has not been implemented all may not be lost. A number of companies specialise in recovery following drive crashes, virus attack, file system corruption and so forth. It might be an expensive exercise but so is data loss. The only solution is to maintain an efficient back-up and recovery strategy and document this in your disaster plan.

Useful websites:

GFS Back-up Strategy http://www.intel.com/support/storageexpress/sb/cs-011789.htm

Data recovery example http://www.ontrack.co.uk

B.10.3 Procuring new information systems#

Any plan to implement new computing facilities or GIS for the HER is likely to begin with staff. This may come about because an existing HER system is coming to the end of its working life or because new technology and improved tools have become available. Once it has been recognised that a new or replacement system is desirable, it is important to prepare a business case for procuring a new system and to specify the HER?s requirements from it.

The HER's parent organisation may have a corporate information systems strategy. This may specify standard software applications to be used within the organisation and for which there is in-house expertise. The strategy document may also give guidelines for procurement of specialist professional applications or for working with IT consultants.

HER databases#

Most organisations consider HER databases to be specialist professional applications that may be developed either as bespoke systems or purchased as off-the-shelf products. In specifying new HER databases it is important to consider both compliance with nationally agreed data standards and user requirements for working with the system. HER managers are recommended to consult other HERs and Historic England (or Cadw in Wales) to discuss the systems that are in use in HERs as well as talking to IT professionals (whether consultants or those working for their organisation).

GIS software#

If a local authority has chosen a particular GIS this may be a powerful argument for the HER to do likewise. A corporate GIS will make the task of sharing data with other sections easier and will enable the HER to harness the expertise within the authority, helping to support the system, and possibly to obtain the software at low or no cost. HER managers should still check that this software meets their requirements. These requirements must be realistic - think about how much a facility would be used, and if the requirement is occasional, whether there are cheaper ways of meeting the need, such as using an external contractor.

One element of the user requirement is likely to be a list of the functions that the GIS is intended to perform. A useful source of advice is the *Functional Requirement Specification for GIS* (LGMB 1991), available from the Improvement and Development Agency, formerly the Local Government Management Board (LGMB). This includes a catalogue of GIS functions, which can be used as a 'checklist' to compare different software products and to assess if any customisation might be required and what skills would be needed to achieve the desired outcome. Target response times for operations that are important to users can provide a useful benchmark and can be used to make sure that the users' expectations and the developer's system performance targets are aligned. For example, if the identification of all records falling within an administrative boundary will be a frequent enquiry what would be the maximum acceptable time for this to take?

Contracts#

If you are entering into a legal contract with an external supplier, it is well worth having a 'health check' from a specialist department, for example legal services or procurement. If internal advice is not available then consider budgeting for specialist advice. The cost may seem expensive, but will be small compared to the expense of a major mistake. Establishing the user requirement and expressing that in legally enforceable terms is a skill in its own right - don't underestimate it!

B.10.4 Data migration#

As data standards and information technology have developed, most HERs have migrated their databases into newer systems. Data migration requires careful planning, which may include:

- completing an audit of the HER database, its data structure and assessing the data quality
- confirming the format in which digital data will be exported from the existing database
- securing a back-up and an archive copy of the existing database
- mapping the data in your old system to the data structure of the new system
- identifying problems or issues with the data to be addressed in advance of migration, including planning, to adopt national data standards and reference data
- planning to complete data migration and have the new system up and running as quickly as possible
- establishing a training programme for HER staff to enable them to become familiar with the new systems.

It is probable that the FISH Interoperability Toolkit will have a significant role to play in the movement and migration of data in the future (See also section B.7).