

# BEBINGTON HIGH SPORTS COLLEGE



# ICT POLICY

Agreed/Reviewed by Governors – see reverse

# **Index**

<b>Policy Scope</b>	<b>Page 3</b>
<b>Appropriate ICT Usage</b>	<b>Page 3</b>
<b>Hardware Acquisition and Disposal</b>	<b>Page 4</b>
<b>Hardware Maintenance</b>	<b>Page 4</b>
<b>Equipment Security and Access Control</b>	<b>Page 5</b>
<b>Data Protection</b>	<b>Page 5</b>
<b>Software Acquisition and Management</b>	<b>Page 6</b>
<b>Backup and Recovery Procedures</b>	<b>Page 7</b>
<b>E mail / Internet usage</b>	<b>Page 10</b>
<b>E-Safety</b>	<b>Page 11</b>
<b>Staff Training</b>	<b>Page 14</b>

## **Policy Scope**

Information and Communications Technology (ICT) is an integral part of Bebington High Sports Colleges administrative and teaching activities: investment in equipment such as workstations, personal computers (PCs) and the communications infrastructure is significant and increasing. ICT is essential to the provision of services and policies and procedures are therefore required to safeguard those services, the school's investment and the effective use of such resources by pupils and staff.

The policy seeks to ensure:

- the physical assets
- access to the information on those assets
- services continuity
- users of the systems and equipment
- compliance with legislation

The policy is applicable to Bebington High Sports College and as such will encompass use of computer resources by:

- all employees including teaching, non-teaching and administrative staff employed by Bebington High Sports College
- all employees and agents of other organisations who directly or indirectly support or use the school's computer systems or networks
- all temporary and agency staff directly employed or indirectly engaged by the school

## **Appropriate ICT Usage**

ICT security is viewed seriously by the school any breach of this Policy could lead to appropriate action being taken against responsible individual(s).

The following examples would be considered as breaches of the policy and inappropriate use of the schools ICT resources:

- the installation and use of unauthorised software
- the installation and use of any unauthorised computer or telecommunications equipment
- unauthorised and/or illicit use of the Internet
- the use of data for illicit purposes
- the copying of software which breaches copyright agreements
- exposing Bebington High School to actual or potential loss (monetary or otherwise) through the compromise of ICT security
- the unauthorised disclosure of confidential or personal information or the unauthorised use of school data
- unauthorised personal use of equipment or changes to equipment configuration
- unauthorised deletion or alteration of files or data
- avoidable damage to the school's equipment
- sharing of passwords or otherwise compromising password security

This list of examples is not intended to be exhaustive.

Any individual who has knowledge of a breach of this Policy must report that breach immediately to his or her line manager as failure to do so could result in disciplinary action being taken.

## **Hardware Acquisition and Disposal**

Hardware expansion and replacement is undertaken in line with the curriculum and administrative requirements of Bebington High Sports College and within the constraints of available finances. All equipment is installed and maintained in line with the currently prevailing Health & Safety legislation. Replacement of major hardware components of the Administration and Curriculum systems was undertaken in 2007 and a programme of replacement and expansion is undertaken on an on-going basis within a time-frame of 4 - 6 years. Curriculum and Administration system hardware and centrally funded departmental ICT provision may be supplemented by individual department acquisitions subject to the availability of departmental funding and technical compatibility with existing provision. Capacity considerations, in terms of both processing and data communications provision will also require consideration when departments are considering independent acquisition of machines and peripheral hardware devices.

Acquired hardware, including PCs, and portable equipment such as laptops and handheld devices will be configured by the System Manager and technical staff or occasionally by departmental staff with their agreement. Systems will be configured to allow users access only to those applications, features and facilities they require to provide the desired functionality and, where possible, these configurations will be standard across workgroups and configured to prevent unauthorised changes. Details of all ICT equipment must be kept on the school's central Inventory system. This is maintained by the System Manager and technical staff, however, the accuracy of the information is a joint responsibility between the System Manager and the purchasing departments. Disposal of any ICT and associated equipment must be carried out in accordance with the prevailing legal requirements with respect to environmental considerations.

## **Hardware Maintenance**

Hardware maintenance contracts with the Wirral LEA Technical Services department provide for a half day per week provision for the undertaking of routine maintenance and support, or the equivalent over an extended period. In the event of serious system failure involving the loss of server capacity, the Wirral LEA provide a 'same day' response to commence problem determination, evaluation and resolution. System restoration will be completed on a timescale commensurate with the nature of the identified problems and will be dependant upon a number of factors including, the complexity of the identified problem and the availability of required hardware components. Bebington High Sports College negotiates and agrees an appropriate service level agreement on an annual basis with the LEA. Copies of this Scope of Work are available within school and by the LEA. Additional support resources may be purchased during the course of the year by mutual agreement if required.

Users have a duty of care to ensure that equipment is not put at risk of damage or theft, and is used in accordance with safe working practices. For example:

- The location of IT equipment should be considered and equipment should be sited to avoid unauthorised access, damage, theft interference and the effects of environmental or other hazards.
- Equipment in transit must not be left unattended.

- Equipment must not be removed or moved to another location without notification being given to the System Manager and technical staff and the appropriate changes made to the central inventory system
- Eating and drinking should not take place in the immediate vicinity of equipment.

## **Equipment Security and Access Control**

All computer equipment is physically secured by means of its location in locked rooms including classrooms, which are only accessible to pupils under staff supervision, with the exception of the Sixth Form Study Area which is monitored regularly by staff. Servers are located in a separate, secured area within the ICT department, which is accessible only to members of ICT department. All teaching rooms are locked when not in use and only accessed when a teacher is present. Administration system workstations are located in areas of the school premises accessible only to staff.

All staff members and pupils have individual user identifiers which are password protected and controlled. The use of another person's user-ID is not permitted. Users must not disclose their user-ID or password or visibly record them on or near equipment providing access to networks or systems. Users must change default passwords, which enable first access, immediately. Passwords must be a minimum of six characters in length, at least one of which must be numeric. Passwords must be changed at regular intervals and especially when it is suspected that the password has been disclosed. The change should be to a previously unused password. Staff who cease to be employed by the school and who have access to applications systems should be removed from the system as soon as possible following the end of their employment.

Password encryption is implemented on all systems and passwords are not held by, or available to, any member of staff. In the event of a user losing or forgetting their password the System Manager and technical staff have a level of access to the system which allows the password to be reset but not retrieved.

Hardware is protected by a labelling system involving the labelling of all equipment by the System Manager and technical staff and the inclusion of all such items in a Central Inventory system of computer equipment, which is held and maintained by the System Manager and technical staff. All computer hardware is audited periodically against the inventory system by the System Manager and technical staff.

## **Data Protection**

All computer programs and data resident on Bebington High Sports College hardware are for the sole use of the school's business and access by staff and pupils is solely for this purpose. Copying, alteration or interfering with computer programs installed on the school's system is not permitted.

Computer based systems within the school which process personal data about living persons must comply with current data protection legislation and should be made the subject of Data Protection registration. There must be no unauthorised disclosure of personal data. Personal data may only be disclosed by the staff who are responsible for the data, with the express permission of the owner, in accordance with data protection legislation. Disclosures must only be made by and to the parties specified on the Data Protection Registration form and in accordance with current data protection legislation.

Key data protection principles include, but are not limited to:

- Personal data must be processed fairly and lawfully.
- Personal data must be obtained only for one or more specified and lawful purposes, and must not be further processed in any manner incompatible with that purpose or those purposes.
- Personal data must be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data must be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose or purposes must not be kept for longer than is necessary.
- Personal data must be processed in accordance with the rights of data subjects under the Data Protection Act.
- Appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against loss or destruction of, or damage to, personal data.
- Personal data must not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedom of data subjects in relation to the processing of personal data.

Virus protection software must be fully implemented and updated regularly, as updates become available, in order to reduce the risks presented to data and systems from this source. This risk is substantially exacerbated by the frequent utilisation of mobile media, including CDs, pen drives and other media by both students and staff. Mobile media which has been used on other PCs, networked or otherwise, within or outside school, must not be used on PCs connected to the school until the media has been checked using appropriate virus checking software. Additionally the school will be connected to the commercial broadband network via a supplementary firewall managed by Wirral LEA Technical Services department.

## **Software Acquisition and Management**

The school licences the use of computer software from a variety of third parties for use within Bebington High Sports College. Additional software is purchased directly from third parties by the school. The copyright of the software will be owned by the software developer and unless expressly authorised to do so, Bebington High Sports College and staff employed therein will not make copies of the software except for backup or archival purposes. The aim of this is to prevent copyright infringement, to protect the integrity of the school's computer environment from viruses and to ensure the efficient management of software.

It is the policy of the school to respect all computer software licences to which it is party. The school should ensure that all staff within the school are aware of this policy and its implications. Staff within school may not duplicate any licensed software or related documentation for use, either on school premises or elsewhere, unless expressly authorised to do so by agreement with the licensor or in agreement with the LEA. Unauthorised duplication of software may subject employees and/or the organisation to both civil and criminal penalties under the Copyright, Designs and Patents Act 1988. Employees may not give or loan software to any unauthorised persons. School employees may use software on local area networks or on multiple machines only in accordance with current software licence agreements.

Software and initial training will generally be budgeted for at the same time as computer hardware. When purchasing software for existing computers, issues such as compatibility with existing software and hardware and network capacity should be determined prior to committing to a software purchase. All such

purchases should be charged to an appropriate budget. When purchasing software staff must follow established organisational purchasing procedures.

All software acquired by the school must be purchased in accordance with the school's ICT development strategy in order that school has a complete record of all software purchased for the school's computers and can register, support and upgrade such software accordingly. All software should be made known to the System Manager or technical staff, who will maintain a register of all the School's software and a library of software licences, with the exception of those supplied and supported by the LEA in which case the LEA shall maintain the library of such software licences.

LEA supplied software will be installed by the LEA and software independently acquired by school will be installed by the Systems Manager and technical staff. The school shall be provided with manuals, tutorials and other user materials as is deemed appropriate. A copy of the applicable licence agreement for LEA supplied software will be held by the LEA and for school purchased software will be held within school. Once installed the original media (and any licence-authorized copies) will be kept in a safe storage area maintained by the LEA or the school as appropriate.

School based computers are organisation assets and must be kept both "software legal" and virus-free. Only software purchased through the procedures outlined above may be used on the school's machines. Staff should not bring software from home, or any other external source, and load it on the school's computers. School software cannot also be loaded onto a member of staff's private computer unless the licence agreement specifically allows this. User profiles allowing access to software resident on the school networked computers will be designed to allow access only to the software required by the user. The profile will be secured so that software access may be controlled and individual users do not have the facility to alter access to software.

School Laptop Computers are organisational assets which are registered to specific, individual members of staff for use in connection with their employment within school and must be kept both "software legal" and virus-free. Only school software purchased through the procedures outlined above may be used on such machines. Employees are only permitted to utilise software from home, or another external source, and load it onto the laptop computer if the registered custodian of the machine holds the license for such software and makes it available for inspection by the school on request.

This is copyrighted software that is distributed freely through bulletin boards and on-line systems, such as the Internet. Only the Systems Manager or technical staff should load Shareware software onto school computer networks, having first taken steps to ensure that such software is virus-free.

An audit of all computers will be carried out at regular intervals to ensure that the school is fully compliant with all software licences. During an audit, a search may be undertaken and any computer viruses found will be eliminated.

## **Backup and Recovery Procedures**

### *System Backup*

Service continuity is a high priority to ensure efficient administration and teaching within the school. It is the joint responsibility of users and the System Manager and technical staff to ensure that appropriate back up and Disaster Recovery procedures are operated and tested. Backing up is undertaken so that if the system fails and the data is lost, a valid current copy of data and software are

readily available for use in the recovery of the system. Software and data hosted on all servers are backed up on a daily basis by the System Manager and technical staff.

Full image back-up is undertaken on each of the five server machines overnight. Each machine is secured to a series of ten backup tapes, three to DAT tapes and two to LTO tapes. Tapes are utilised on three separate cycles to facilitate the retention of secured systems on a daily, weekly and quarterly basis. Backups created on Monday – Thursday nights are overwritten on a weekly basis, Friday night securities created on the first three Fridays of the cycle are retained for four weeks from the date of creation and overwritten in rotation and the Friday night backup copy created on the fourth Friday of the cycle is retained for twelve weeks to create a quarterly security copy. In addition to the above cycles a copy of backup created at the end of the Summer term (end of July) is withdrawn from the cycle and retained for a full calendar year as an annual archive. The timing of the annually retained backup is scheduled at this point in the calendar to achieve the maximum retention of completed coursework for a complete year from the curriculum network and as a checkpoint year end from the administration network.

Daily backup copies are stored off-site overnight in order that any disaster occurring during the overnight period, whilst school buildings are empty, can be recovered using the off-site backup copies. In the event of a failure of any or all of the overnight backup processes the backup routines are initiated and run by the System Manager and technical staff at the start of the following day and the reason for the failed backup process investigated and reported to Wirral LEA Technical Services department as required. During the day, prior to the removal of backup tapes for overnight off-site storage, tapes are located in a specified location in the server room and will be removed from the building if an evacuation of the building takes place during the school day by the System Manager, technical staff or ICT co-ordinator. The weekly security copy of the Administration system is secured in a safe in the Server room adjacent to F16.

The tape drives utilised for the backup of systems are cleaned on a weekly basis or on prompting dependant upon the tape drive to ensure effective data security. Self-cleaning AIT tape drives require the use of a cleaning tape once a year.

### *Disaster Recovery*

Disaster recovery will be implemented to varying degrees in accordance with the severity of the situation encountered. The following are examples of scenarios which would trigger the implementation of Disaster Recovery procedures:

- Damage to premises including loss of one or more servers and network machines
- Loss of one or more servers, but not damage to the associated network machines
- Loss of a number of network machines, without the loss of a server
- Loss of network capability in all or part of the school premises
- Loss of major network components

Isolated damage occurring to single workstations is not considered to constitute a disaster and will be resolved within the school's normal ICT maintenance procedures.

## *System Restoration Procedures*

Dependant upon the nature of the disaster scenario it is possible that prior to the restoration of computer systems alternative accommodation for servers would have to be agreed with the facilities management company responsible for school maintenance. If a file server becomes irrevocably damaged it may be replaced under the terms of the school's current insurance policy and the systems and application software will be re-installed by Wirral LEA Technical Services department under the terms of the current service contract. School based data and software will be restored from the backups held on tape, to the point in time at approximately midnight of the day prior to the disaster occurring. Backups will not normally exist beyond this point in time.

### *Order of systems restoration*

The School's Administration System is regarded as the highest priority system in terms of restoration due to its impact upon the business and administrative functions of the school. Restoration and reconfiguration of this system will take place in accordance with the following sequence:

- Replacement and reconfiguration of server hardware
- Restoration of an effective network system
- Installation of Operating System Software
- Installation of the basic SIMS application software
- Restoration of SIMS data files to last secured point
- Installation of the Microsoft Office applications software
- Installation of Pupil Management applications software
- Restoration of data files to last secured point

The Curriculum System may be reconfigured concurrently with or subsequent to the Administration System, dependant upon the degree of damage and the available resources for the completion of the process. The Curriculum System will be reconfigured in accordance with the following sequence:

- Replacement and reconfiguration of server hardware
- Restoration of an effective network system
- Installation of Operating System Software
- Installation of the Microsoft Office applications software
- Installation of additional teaching applications software packages
- Restoration of data files to last secured point

Replacement hardware in the event of system failure will be provided by the Wirral LEA Technical Services department in line with the current service contract but will be subject to availability of hardware. Rebuilding of server machines in the event of failure will be undertaken by Wirral LEA Technical Services department in line with the current maintenance contract and will normally require one working day per machine, subject to the availability of components and suitably skilled staff resources.

The responsibility for the replacement or repair of components resident within the main switch cabinet lies with the networking section of Wirral LEA Technical Services department but access and timescales would be subject to negotiation with the facilities maintenance provider (Hochtief). Satellite communications cabinets are subject to the same process in order to restore service but the impact would be limited to within the vicinity of the affected cabinet / communications equipment.

The initial point of contact in the event of a disaster will be the System Manager who will co-ordinate the systems recovery procedures and contact other personnel as required. This will include LEA Technical Support section, Network providers, Site Manager, Building maintenance personnel and other personnel who may be involved in the restoration of a functioning service. The ICT Co-ordinator and System Manager will also be responsible for keeping staff within school informed of the progress of the recovery procedures. The Head Teacher will be kept fully apprised of the situation at all times.

(Contact telephone numbers for all these people to be held with the DR plan in the Main School Office and in an off-site location)

1. Backup tapes are held on the school premises in a secured area within the ICT department. There will be a copy of all machine backups held off-site overnight so that if the backups held within school become damaged there is always a viable set of tapes available.
2. The Systems Manager will locate the latest backup tapes and ensure that these are undamaged and viable for the purposes of system restoration.
3. If a return to normal computer service will take some time to achieve, manual procedures will have to take their place for a while. The administration function will proceed with the maintenance of paper based records, which will be retained securely and entered onto the administration system to bring it to a state of currency on completion of the system restore, when functioning system is returned to staff by the System Manager.

The loss of the curriculum system will mean that all lessons within school which are normally delivered by means of ICT based resources will be replaced with classroom based, non ICT lessons, until such time as the system becomes available for use.

The Disaster recovery plan will be held in the ICT department, with additional copies kept securely in the School Office and one copy off-site at the home of the System Manager.

## **E mail / Internet usage**

Members of staff, pupils and all other users including Governors are required to follow all conditions laid down in this policy. Staff and Governors must complete and return the Internet Agreement included at Appendix A and pupils and parents must complete the agreement at Appendix B prior to gaining access to the school's computer system. Any breach of these conditions may lead to withdrawal of the user's access to the school's computer systems and in extreme instances of misuse, criminal prosecution. In the case of employees, a breach may also be considered a breach of the employee's conditions of service, which could lead to dismissal on the grounds of gross misconduct.

Use of the Internet and facilities such as the electronic mail service are intended for educational purposes only. To help protect pupils from unsolicited email no pupil is directly identifiable by his or her email address. The schools equipment and the Internet may only be used for legal activities consistent with the aims, objectives and rules of the school.

The following activities, whilst not an exhaustive list, are examples of deliberate and unacceptable use of the Internet:

1. The access to or creation, transmission or publication of any offensive, obscene or indecent images, sounds, data or other material.

2. The access to or creation, transmission or publication of any data capable of being displayed or converted to such obscene or indecent images, sounds, data or other material.
3. The creation, transmission or publication of any material designed or likely to cause offence, inconvenience or needless anxiety.
4. The creation, transmission or publication of defamatory material.
5. The receipt or transmission of material which infringes the copyright of another person or infringes the conditions of the Data Protection Act 1984.
6. The transmission of unsolicited commercial or advertising material to other users.
7. The deliberate unauthorised access to facilities, services, data or resources within the Wirral Learning Grid or any other network or service accessible via the Internet.
8. Deliberate activities with any of the following characteristics or that by their nature would result in:
  - Wasting staff or other users efforts or network resources, either in school or elsewhere.
  - Corrupting or destroying other users data.
  - Violating the privacy of other users (e.g. Data held on a network).
  - Disrupting the work of other users whilst they are using the equipment in school.
  - Using the Internet in a way that denies service to other users (for example, by overloading the connection to the network by unnecessarily, excessively and thoughtlessly downloading large files including multimedia files).
    - Continuing to use any item of software after being requested to cease its use because it is disrupting the correct functioning of the school's network or the Wirral Learning Grid or the Internet (for example, software designed to broadcast messages to all users of the Network).
    - The deliberate introduction of "viruses" to the Network.
9. Where the Internet is being used to access another network, any abuse of that network will be regarded as unacceptable.
10. Any use of the Internet that would bring the name of the school or the Local Authority into disrepute.
11. The school's personal computers (including portables) must only be used to access the Internet through an officially authorised route.
12. The user should only print essential resource material and should always check that the length of a document is reasonable before printing.

## **E-Safety**

This e-safety and acceptable use policy has been written using Becta guidance. It will be reviewed in accordance with those guidelines on a regular basis.

ICT has a critical role in equipping students for life in the 21st Century and ICT can have a positive impact on teaching and learning. To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom. The intention of this policy document is to protect all parties – the students, the staff and the school, and aims to provide clear advice and guidance on

how to minimise risks and how to deal with any infringements.

### *Staff Responsibilities*

All staff are responsible for promoting and supporting safe behaviours in their classrooms and for following e-Safety procedures. Staff should also be aware of their personal responsibilities to protect the security and confidentiality of the school network.

The Green Paper, *Every Child Matters*<sup>1</sup> together with the provisions of the *Children Act 2004*<sup>2</sup> and the policy document *Working Together to Safeguard Children*<sup>3</sup> sets out how organisations and individuals should work together to safeguard and promote the welfare of children.

The 'staying safe' outcome includes aims that children and young people are:

- safe from maltreatment, neglect, violence and sexual exploitation
- safe from accidental injury and death
- safe from bullying and discrimination
- safe from crime and anti-social behaviour in and out of school
- secure, stable and cared for.

These aims apply equally to the virtual world that children and young people will encounter whenever they use ICT in its various forms. For example, there is a need to protect students from dangers such as:

- the use of the internet for grooming children and young people with the ultimate aim of exploiting them sexually
- the use of ICT as a new weapon for bullies, who may torment their victims via websites or text messages
- exposure to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour.

It is the duty of all staff to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

### *To Ensure Security & Confidentiality*

- Maintain password security. Passwords should not be shared with any other member of the school community, nor should they be written down.
- Staff laptops must also be password-protected.
- When unattended, computers must be logged off or locked down. This is equally applicable in classrooms, departmental areas and in offices.
- All computers and associated equipment must be shut down and turned off at the end of the day.
- Data storage devices such as USB pens, portable hard drives, CD-Roms and DVD-Roms must be subject to virus protection measures by 'stopping' devices before removal from the computer, and not inserted in the first instance if the source cannot be trusted.
- Any accidental access of inappropriate material on the internet should be reported to staff. The school reserves the right to examine internet access logs from any computer in the school and staff laptops issued by the school. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.
- E-mails from suspicious sources should not be opened. These should be reported to the System

Manager. Software should not be downloaded unless the source can be trusted and the member of staff has checked that there is no infringement of licensing laws.

- Photographs of students should only be taken and saved on the network where permission to do so has not been denied by parents.

### *To safeguard the facilities and support student behaviour*

Vigilance by staff in supervising and monitoring student use of ICT will reduce the incidence of damage to expensive resources and help to secure e-Safety for the students. The expectations of students are clearly described in the 'ICT Student Agreement.' Expectations of staff are described below:

- Students must always be supervised in ICT suites and in classrooms where laptops are in use. The doors should be locked in the absence of a member of staff.
- Upon discovery, all damage must be reported immediately.
- Seating plans must be used to ensure that any subsequent damage can be tracked to individual students.
- Ceiling projectors must be turned off when they are not in use by using the remote control.
- Food and drink must not be consumed in ICT suites or in classrooms where laptops are in use.
- Portable laptops used in lessons must be returned to the trolley and locked after use by a class.
- Students should not be given access to electrical equipment if they have wet clothing.

### *How will complaints regarding e-Safety be handled?*

The school will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- Interview, counselling and/or disciplinary action by class teacher, Year Manager, ICT Coordinator or Head Teacher
- informing parents or carers
- removal of Internet or computer access for a period
- referral to LEA / Police.

Any complaint about staff misuse will be referred to the Line Manager and ultimately to the Head Teacher and may result in formal disciplinary proceedings.

Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LEA child protection procedures.

## **Staff Training**

Administrative staff are trained in the utilisation of the systems and software packages as appropriate and as an integral part of the introduction of any new system functionality. Curriculum development is an ongoing process and associated training will be carried out using training services available from within the LEA or from external organisations as appropriate.