



ASHLAWN SCHOOL
'A High Performing Specialist Academy'

E-SAFETY & ICT NETWORK POLICY

Policy & Procedure Number		AP020				
Date Approved for use by The Governing Body						
Next Review Date		1 st February 2018				
School Link		K Smith				
Acknowledged & signed by	Headteacher					
Acknowledged & signed by	Chair of Governors					
Circulation	Internal	✓	External	✓	Website	✓
<i>PRINTED COPIES ARE UNCONTROLLED</i>						

This policy needs to be read in conjunction with the Safeguarding Policy

Contents

WHAT IS ICT?	1
ICT RESOURCE PROVISION AT ASHLAWN	2
General points	2
Purchasing and procurement	2
Repairs, upgrades and maintenance	3
Use of external support agencies	3
Allocation and maintenance of consumables	3
Backing up of files	3
USE OF THE NETWORK	3
Student access to the Network	3
Removal of access rights for students	3
Internet access for students	4
Staff access to the Network	4
Laptop trolleys and allocation of laptops during lessons	4
Staff use of the Internet and VLE	4
Staff use of e-mail	5
Booking resources	5
SOFTWARE AND LICENSING.....	5
The purchase of whole school, generic software applications	5
Removal of unwanted or out of date software	5
Demo, shareware, Beta or trial software	5
MONITORING AND REVIEW OF THIS DOCUMENT	6
APPENDIX A.....	7
Guidelines for use of computer rooms	7
Appendix B	8
Acceptable Use Policy – To be signed by all students	8
APPENDIX C.....	10
E-SAFETY POLICY	10
Staying safe online – Ashlawn’s E-Safety Policy	10
Staying safe online – managing content in school	10
Staying safe online – teaching responsibility	10
Staying safe online – responsibility of teachers	10

APPENDIX D 11

SAFEGUARDING IN A DIGITAL WORLD 11

SCHOOL CORE POLICY 11

What is ICT?

Information Communication Technology is much more than just another subject within the National Curriculum. It is also a tool by which we can enrich the learning experience within all other subjects. It is also much more than just Information Technology (IT) with a new name. It includes 'communication' or more accurately 'collaboration', making use of the many ways in which we exchange and share information with the world around us.

It is about equipping the young people of today with the tools to face the challenges of an increasingly technological world of tomorrow.

The teaching and learning of ICT is therefore paramount to the development of students at Ashlawn School. The learning of ICT can be thought of in three levels:

*Level 1 - Learning **about** ICT*

Teaching the skills and processes associated with the use of ICT equipment, learning how the icons and menus work, very little learning of subject material takes place.

*Level 2 - Learning **with** ICT*

Using the skills and tools gained during level 1 to access learning about a particular topic, e.g. using a CD-ROM to find out about famous inventors, accessing the Internet to research historical information about World War Two etc. This type of learning would still be possible without the use of ICT tools.

*Level 3 - Learning **through** ICT*

Using ICT to experience learning that would not be possible otherwise; e.g. analysing molecular structure through a computer generated model, observing the results from data sensors when dealing with very short or very long periods of time.

In order to enrich the learning experience by taking full advantage of the range of ICT tools and processes, it is important that we develop a culture of learning **through** ICT within other faculties.

Students acquire skills in a number of key ICT areas making use of standard applications (word processing, databases, spreadsheets, graphics and desktop publishing) as well as using new technologies like digital imaging and manipulation, video and sound editing, computer control and data logging. In addition, they collaborate using e-mail and the Internet.

The rapidly changing nature of the subject means that it is important that we keep up to date with developing technologies, and as these become available it is our vision to embed these into the curriculum.

This document is therefore an important vehicle by which this can be achieved and therefore improve the learning experience for all students.

ICT Resource provision at Ashlawn

General points

ICT at Ashlawn is provided using PC machines running Windows operating systems and generic software applications. The school aims to make its provision of ICT follow that of industry and higher education in order to allow students the opportunity to experience this kind of provision. The vast majority of machines are networked in order to facilitate students' use of ICT in many areas of the school. *The school provides these machines for purposes relating to the educational development of its students and professional use made by its staff and provides access to this resource **for that purpose solely.***

ICT resources are provided in a number of cluster areas or suites which are initially the responsibility of the individual departments in which they are located. Most cluster areas are equipped with access to a printer for hard copy output of work, some have other peripherals.

Staff using these areas with students are responsible for the management of that area during the time of the lesson and should follow the guidelines laid out for that room. Copies of the guidelines for each room are included in the Appendix.

Equipment faults, empty toner or ink cartridges or other problems encountered in the room should be reported to the Network Manager and/or IT support team using the procedure outlined in this document.

Other resources are provided for use within the school, these include digital projectors, air-writers, laptops, wireless keyboards and mice, interactive whiteboards, digital stills and video cameras. Initial responsibility for the management of these items is with the member(s) of staff to which they have been allocated. For all new allocations, staff will be asked to sign to acknowledge this. Records of serial numbers will be collected and added to the Asset Database which is held and updated by the Network Manager.

Purchasing and procurement

The school aims to provide high quality, cost effective ICT provision for its students and staff. The cost centre manager for whole school ICT will endeavor to find the most competitive quotations from reputable companies, and is not tied to one particular provider. The school aims to achieve a computer to pupil ratio which is better than national and local targets whilst ensuring quality, up to date and reliable equipment.

All capital purchases between £1000 and £10,000 will be made by gaining competitive quotations from at least three reputable companies before making a final decision. Purchases above this figure will go to tender and seek governor approval before a decision is made.

The initial need for new purchases will most likely come from department and whole school development plans where key areas of ICT development are identified and costed. These needs are fed to the ICT cost centre manager who, in consultation with the Network Manager and Head/SLT will decide upon the priorities, based upon current needs and direction. In some situations it may be necessary to convene other groups in order to look at the proposals.

The school aims to maintain a consistently high standard of equipment provision by constantly reviewing and replacing hardware which does not meet the minimum required specification.

Repairs, upgrades and maintenance

It is primarily the job of the Network Manager and IT Support team to ensure that equipment is kept working and available for student and staff use whenever required.

Requests for ICT work will be made by emailing or calling the helpdesk. *A working solution or response and timescale for the issue will be given to the member of staff making the request within **24 hours** of the IT Support team receiving it.* Copies of these requests will be retained on the system.

The Network Manager and IT Support Team will keep an ongoing journal of current jobs which will be available for the ICT Cost Centre Manager to monitor at regular intervals. This journal will be retained once full to allow reference to be made to previous jobs and solutions applied.

Allocation of software installed within suites will need to be made **at least** half a term in advance to allow the Network Manager and IT Support team to carry out the work during school holidays giving sufficient time for installation, allocation and testing. Similarly, all major ICT maintenance, repair and upgrade requests will need to be made **at least** half a term in advance wherever possible, again to allow sufficient time for the work to be carried out and testing to take place. Requests for installation to individual PCs and laptops will need a reasonable notice period of **no less than one week** before it is required. Staff requiring installation/configuration of laptop software should be aware that their laptop will not be available during this period and they should seek advice about alternative arrangements.

All urgent ICT requests must relate directly to whole school strategic plan or departmental priorities for them to be carried out with less than the minimum required notice. The Network Manager and IT Support team will ascertain the priority and required timescale for these maintenance requests and will give an estimated completion date to the relevant member of staff.

Use of external support agencies

The ICT Cost Centre Manager will continue to monitor the quality of service provided by these providers and will review the contract annually in order to provide the school with the best quality of service.

Allocation and maintenance of consumables

It is the responsibility of the Network Manager with the support of the IT Support Team to maintain a reasonable stock level of printer consumables to ensure that the amount of time when printers may be without ink/toner is negligible.

Backing up of files

A full backup of each server will take place each night and indexed to provide at least one full week's backup to enable restoration of lost files. In addition, one archive will be created each month of the Admin Server to provide a permanent backup of finance and SIMS information.

Use of the Network

Student access to the Network

A new user area will be provided for each new student joining the school. Students will be allocated a standard desktop, standard access privileges and sufficient file space. This user area is the responsibility of the student to maintain for purposes relating only to the courses of study followed by the student. *The school stresses that the network is provided as an educational tool and should be used as such by the student.* Students are allowed to save documents and files created *only* by the applications provided by the network. Students will be encouraged to follow good practice with regard to file management; naming files appropriately, creating suitable subdirectories and deleting unused files when no longer required.

Students will be required to read and sign the student ICT contract (Included in appendix) which explains the expectations for student use of the Network.

Removal of access rights for students

Where a student's use of the network is felt to be contrary to the contract, they should be referred directly to the ICT Cost Centre Manager/Member of SLT who will ascertain the nature and severity of the incident. Under the direction of the ICT Cost Centre Manager; the Network Manager may also issue sanctions. Appropriate sanctions including the removal of access privileges will be enforced with the

support of the relevant Head of Year and in more extreme incidents, the Headteacher. The school acknowledges that removal of access privileges may occasionally be inappropriate as it may cause further problems with the student being unable to participate in lessons and being unable to complete coursework. Staff will endeavor to find the most appropriate course of action for each incident.

The school has no intention to ban students at every opportunity but to restrict access whilst educating the individual in the correct etiquette, thus preventing repeat offences.

The Network Manager will keep a record of a student's misdemeanors on the network for the length of time that the student remains an active user of that network. This will be for the purpose of keeping a log of repeat offenders and spotting patterns in offences etc.

Internet access for students

All students will also be issued with access privileges to the Internet via the school's default browser. The school provides this resource for purposes relating to education and the student's courses of study only. Further detail surrounding the school's Internet provision can be found in the separate Internet and VLE Policy document.

Staff access to the Network

All staff (where appropriate) are provided with access to the school network. They will be allocated a staff desktop and access to resources appropriate for their role.

Additional privileges and allocations are at the request of the member of staff with the agreement of the ICT Cost Centre Manager under the direction of the Headteacher.

Staff will be provided with sufficient file space which is their responsibility. The use of this is at the discretion of the member of staff, provided it goes no way to compromising the integrity or performance of the network. Therefore staff should respect the fact that *the network is provided as an educational tool for purposes relating directly to the operation of the school.*

Staff requiring resources or services not provided by the network should first consult with the ICT Cost Centre Manager who, in conjunction with the Network Manager and in some cases the Head will ascertain the appropriateness of the request.

Staff will be encouraged to follow good practice for file management with naming of files and creation of suitable subdirectories. In addition, the ICT Cost Centre Manager will request staff delete old and redundant files on a regular basis to retain server space. Archive DVDs can be created if requested by members of staff.

When a member of staff is leaving, the contents of their network area will be copied onto CD/DVD and given to them. Their area will be left available for a period of **one term** before being removed by the Network Manager or IT Support Team thus regaining server space. Email addresses and user logins will be disabled from the first day after the member of staff has left, or at the discretion of the Head.

Laptop trolleys and allocation of laptops during lessons

Staff may wish to book a trolley of laptops for use during their lesson or a number of individual laptops. Staff should know that *they* are responsible for the laptops they have booked and in the case of any loss or damage, *their department* may be liable for recompense if **due care** has not been seen to have been followed.

Therefore it is important that all laptops allocated to students are checked at the beginning and end of each session; and your expectations for their use is made clear to students at the beginning of the session. Teachers must keep a record of which laptop is allocated to each student to aid investigation of any issues later.

Staff use of the Internet and VLE

Staff will also be provided with access to the Internet and VLE via the school's Internet Provider and default browser. The use of this resource should be in accordance with the school's Internet and VLE Policy.

Staff may be given additional access to sites which are filtered by the default filtering preferences if it is mutually felt by the ICT Cost Centre Manager and the member of staff that the site in question is appropriate within the school context. In addition, staff may also request to have sites filtered if they feel the content is unsuitable for school use.

Staff use of public domain sites and social networking sites.

Whilst staff use of the Internet from home is not within the bounds of this document, it is worth mentioning that where staff associate themselves with Ashlawn School on public domain sites and social networking sites they should be aware of the need to uphold the professional reputation of the school and themselves. Always consider the audience and consequences of using these sites.

Staff use of e-mail

Staff will be issued with an email address provided with an '@ashlawn.org.uk' suffix. Staff will be expected to use this as their default professional e-mail account. Staff should not use any other account with regards to the school's professional business. Staff who wish to use email to receive work from students should request an alias email account, e.g. Englishteacher@ashlawn.org.uk.

Booking resources

Staff may book resources to be set up for use in lessons, meetings and assemblies. This would ordinarily mean laptops, projectors etc. This should be organized via the IT support team with reasonable notice and clear instructions given. Therefore the minimum expectation is for **at least 48 hours** notice be given for all such bookings to ensure availability and the following information to be made available; staff making request, date, time and length of booking, venue and equipment required. This will ensure that staff needs can be met more effectively and where equipment is not available, alternative solutions can be offered.

Software and Licensing

The purchase of whole school, generic software applications

The ICT Cost Centre Manager, along with the Network Manager will be responsible for the purchase and upkeep of all software on the school network. This will be in accordance with procurement policy stated previously. This will include the following:

- Operating systems (both workstation and network)
- Utilities and tools (such as anti-virus etc.)
- Generic software applications (such as integrated office applications)
- Subject specific software (as used in faculties to support curriculum activity)

It is the responsibility of the ICT Cost Centre Manager under direction by the Headteacher to ensure that sufficient licenses are obtained and kept up to date and available. Where software is to be used by specific areas of the school, it is primarily the responsibility of the member of staff who purchases the software to ensure that sufficient licenses are obtained. When both the ICT Cost Centre Manager and Network Manager are satisfied that sufficient licenses are available for allocation to the required numbers of workstations, the software will be installed.

The school will not install or run software which is unlicensed or where insufficient licenses are available.

Where faculties purchase their own subject specific software, the original CD (or equivalent) will be kept by the Network Manager along with the License agreement. A copy of the license may be retained by the relevant faculty for their own records.

Removal of unwanted or out of date software

The Network Manager will undertake an annual review of the software and license provision and will recommend the removal of surplus software. Individuals concerned will have the opportunity to renew license agreements or have the software removed.

Demo, shareware, Beta or trial software

These types of software may be used only under the terms of their documentation and for no longer than the time permitted. In addition, software deemed to be for stand-alone use only will not be installed onto

the network if a dedicated network version is available, even if sufficient licenses are gained. Only software which is designed to be run on the school network will be installed.

The Network Manager and IT Support Team, under the direction of the ICT Cost Centre Manager are the only persons authorised to install software onto the school computers. Any other attempts may be damaging to the network and will be seen as a misuse of the Network resource.

Monitoring and review of this document

The effectiveness of this document will be reviewed by the ICT groups as specified previously. They will recommend any revisions during the course of its life which will be one year.

Each year, the ICT Cost Centre Manager will review the policy document to ensure it remains up to date and covers any recent developments which may have an impact upon ICT within the school.

It is also the responsibility of the ICT Cost Centre Manager to ensure dissemination of this policy to all relevant parties and to administrate its implementation.

Appendix A

Guidelines for use of computer rooms

Guide for staff using computer rooms

General rules:

- Coats or bags brought into the room must be placed at the central tables. If placed under the computer desks, these could become entangled on wires underneath desk and result in cables being pulled out.
- Under no circumstances should food and drink be near computers. In classrooms, students should only be allowed to drink water in the centre of the room, as far away from computers as possible.
- Students will be liable for the replacement costs of any equipment damaged.

During the lesson:

- At the beginning of a session ask students to check that the computer is in good working order.
- Students should check their print preview before each print in order to cut down on wasted paper.
- Students should be reminded to save work every 10 minutes or so.
- Students should be encouraged to proof read and spell check on screen before printing.
- Students should be reminded of the Acceptable Use Statement displayed in the room.

If things go wrong:

- Don't panic - it's probably not your fault!
- Call the ICT Support Team on 415.
- Email: helpdesk@ashlawn.org.uk

At the end of the lesson:

- Students should log off the machines and check to see if they have left anything behind (including any print-outs, scrap paper, pens etc.)
- Check there is sufficient paper in the printer for the next class.
- Ensure that each machine is as it should be. (Check mice, keyboards etc.)

At the end of the day:

- Students should log off and then shut down each of the machines.
- A final check should be made that nothing has been left by the side of each machine.
- Ensure that each machine is as it should be. (Check mice, keyboards etc.)

Carrying out these simple checks ensures all rooms remain in good working order

Appendix B

Acceptable Use Policy – To be signed by all students



Ashlawn School - Acceptable Usage Policy - Curriculum Computer Network

The School provides computers for use by students. They offer access to a vast amount of information, acting as an extension to the school library and offering great potential to support the curriculum.

The computers are provided and maintained for the benefit of all students, who are encouraged to use and enjoy these resources, and ensure they remain available to all. Pupils are responsible for good behaviour on the internet, just as they are in a classroom or when using a school corridor. Access is a privilege, not a right and inappropriate use will result in that privilege being withdrawn.

In order to ensure that the computers remain fully operational, we all have to abide to some guidelines. Please read through the following guidelines carefully and sign the bottom of the sheet to say that you understand and agree to these conditions.

Once it has been signed and returned to the Network Manager, you will be given a username and password. If you break these rules, access to the network will be withdrawn and disciplinary action will be taken.

Additional action may be taken by the school in line with existing policy regarding school behaviour. For serious violations, a period of exclusion or even permanent exclusion may be imposed. Where appropriate, police may be involved or other legal action taken.

Equipment

- Do not install, attempt to install, execute or store programs of any type on the computers without written permission.
- Do not damage, disable, or otherwise harm operation of computers, or intentionally waste resources.
- Do not use computers for commercial purposes, e.g. buying or selling goods.
- Do not open files brought in on removable media such as floppy disks, CD's flash drives etc until they have been checked with anti virus software and found to be clean of viruses.
- Do not connect mobile equipment to the network e.g. laptops, tablet PC's, PDA's etc until they have been checked with anti virus software and found to be clean of viruses.
- Do not eat or drink near the computer equipment.

Security and Privacy

- Do not disclose your password to others, or use passwords intended for the use of others.
- Never tell anyone you meet on the internet your home address, your telephone number, your schools name, or send them your picture.
- Do not use the computers in a way that harasses, harms, offends or insults others.
- Respect and do not attempt to bypass security systems in place on the computers, or attempt to alter any of the settings.
- Computer storage areas and removable disks will be treated like school lockers. Staff may review files, and communications to ensure that users are using the system responsibly.
- Do not log on to other students accounts even if they give you their permission.

Internet

- Do not access the internet unless for study or for school authorised/supervised activities.
- Do not use the internet to obtain, download, send, print, display, or otherwise transmit or gain access to materials which are offensive, unlawful, obscene or abusive.
- Respect the work and ownership rights of people outside the school, as well as other students or staff; this includes abiding by copyright laws.
- Do not engage in "chat" activities over the internet.
- Never arrange to meet anyone you have met online. People you contact online are not always who they seem.
- Never attempt to access by other means sites blocked by the schools security system.

Email

- Be polite and appreciate that other users might have different views from you own. The use of strong language, swearing or aggressive behaviour is not allowed.
- Never open attachments to email unless they come from someone you know and trust. They could contain viruses or other programs which would destroy all the information and software on your computer.
- The sending and receiving of email containing material likely to be unsuitable or inappropriate is strictly forbidden. Always report such messages to a member of staff.

I have read and understood the above and agree to use the computer facilities within these guidelines.

Signed _____ Print Name _____ (Student)

Signed _____ Print Name _____ (Parent/Guardian)

Appendix C

E-Safety Policy

Staying safe online – Ashlawn’s E-Safety Policy

Ashlawn School has adopted the *Warwickshire Core E-Safety Policy* Appendix D. Additional detail is also included below.

Staying safe online – managing content in school

Students are granted access to the Internet via a secure and filtered account at Ashlawn School. This is provided, recommended and supported by Warwickshire LA. Logs of all internet activity are kept and retained in the event of e-safety related issues. Filtering is managed by the Network Manager who is CEOP trained and can identify and respond to issues which may arise.

Staying safe online – teaching responsibility

Whilst these procedures are in place we recognise that the primary safeguarding method is one of education and so students are educated in staying safe online through the following:

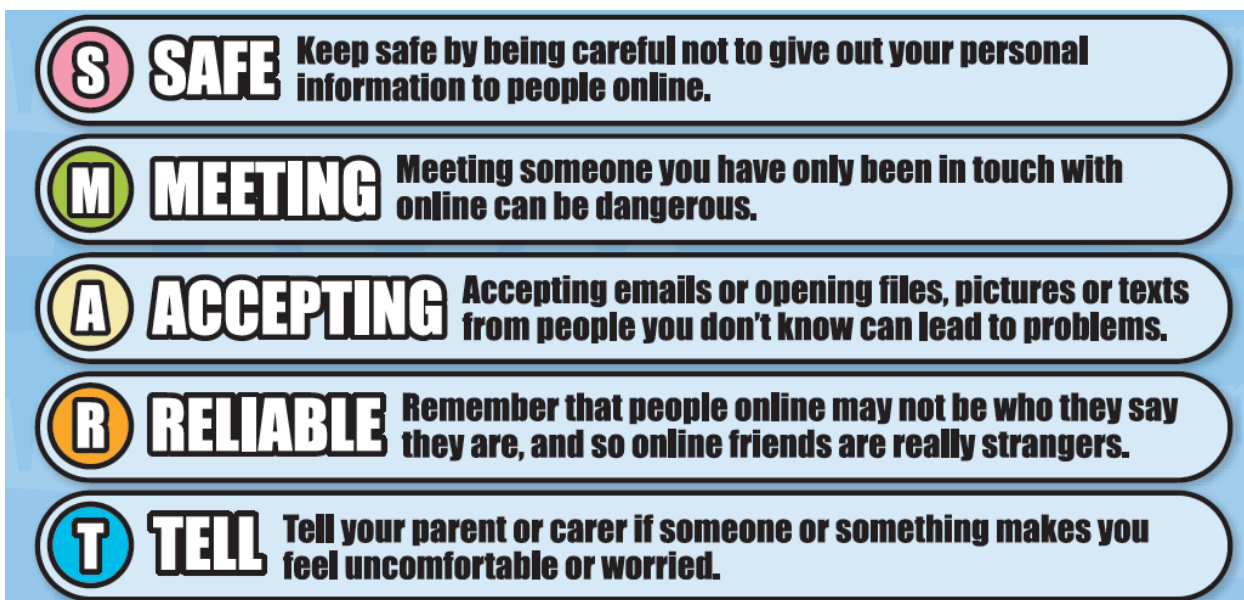
- Annual E-Safety assemblies for all
- As part of Year 7 ICT schemes of work for all students
- Through PSHE SOL in other years
- As part of Y9/10/11 Dida work for ICT students
- Annual renewal of ICT Acceptable Use Policy (AUP) signed by students
- As part of work of pastoral team, as and when necessary in response to incidents

Staying safe online – responsibility of teachers

Teachers are directed to be aware of the AUP and its implications. Teachers are directed to look out for and pass on any instances students breaking the AUP or putting themselves at risk online. This may be within school or outside of school. Issues must be reported to the designated Child Protection Officer and/or ICT Cost Centre Manager as appropriate who then acts within the scope of their role.

Staying safe online – Staying SMART

Students are safeguarded using a range of materials as part of the list above. Through all of this, the key message is that students should be SMART online:

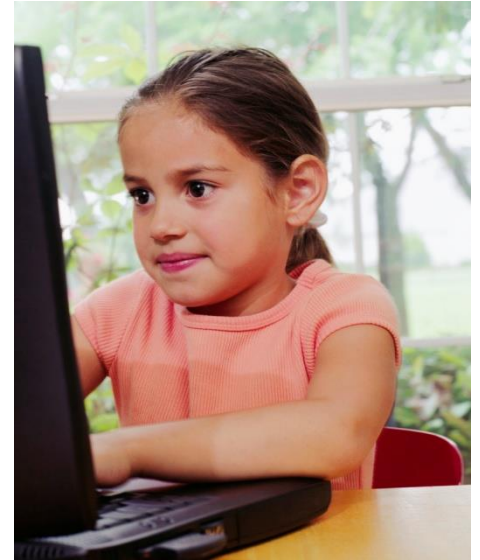




Safeguarding in a Digital World

School Core Policy

Warwickshire ICTDS has approved this core e-Safety Policy which could be used by Warwickshire schools as the basis to construct their own policy.



The requirement to raise awareness in children, young people and adults of the risks associated with inappropriate contact and behaviour via the internet and access to inappropriate content on the internet is addressed as part of the wider duty of care for all teachers. It is essential that all pupils are taught the relevant skills and strategies to remain safe when using the internet and related technologies, and that they use these technologies appropriately. This may be as discrete internet safety lessons, as part of the ICT curriculum, and embedded within all curriculum work wherever it is relevant. Recognising the issues and planning accordingly will help to ensure appropriate, effective and safe use.

John Parmiter
Head of ICT Development Service
Children, Young People & Families Directorate
Warwickshire County Council

September 2009



In Support of
Learning



ICT Development
Service

Writing and reviewing the e-safety policy

The e-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT and for child protection.

- *Our e-Safety Policy has been written by the school, building on the Warwickshire ICT Development Service e-Safety Policy and government guidance. It has been agreed by the senior management and approved by governors and the PTA.*
- *The e-Safety Policy will be reviewed annually.*

Teaching and learning

Why Internet use is important

- *The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.*
- *Internet access is an entitlement for students who show a responsible and mature approach to its use.*
- *Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.*

How does Internet use benefit education?

Benefits of using the Internet in education include:

- *Access to world-wide educational resources including museums and art galleries;*
- *Inclusion in the National Education Network which connects all UK schools;*
- *Educational and cultural exchanges between pupils world-wide;*
- *Vocational, social and leisure use in libraries, clubs and at home;*
- *Access to experts in many fields for pupils and staff;*
- *Professional development for staff through access to national developments, educational materials and effective curriculum practice;*
- *Collaboration across support services and professional associations;*
- *Improved access to technical support including remote management of networks and automatic system updates;*
- *Exchange of curriculum and administration data with the LA and DfES;*
- *Access to learning wherever and whenever convenient.*

Internet use will enhance learning

- *Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.*
- *Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.*
- *Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.*

Pupils will be taught how to evaluate Internet content

- *If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to Warwickshire ICT Development Service, and where appropriate the school e-safety officer.*
- *Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.*
- *Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.*
- *Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.*
- *The evaluation of on-line materials is a part of every subject.*

Managing Internet Access

Information system security

- *The security of the school information systems will be reviewed regularly.*
- *Virus protection will be installed and updated regularly.*
- *The school uses the Warwickshire Broadband with its firewall and filters.*
- *The school provides an addition level of protection through its deployment of Policy Central in partnership with Warwickshire ICT Development Service.*
- *Portable media may not used without specific permission and a virus check.*
- *Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.*
- *Files held on the school's network will be regularly checked.*
- *The ICT co-ordinator/network manager will review system capacity regularly.*

E-mail

- *Pupils may only use approved e-mail accounts on the school system.*
- *Pupils must immediately tell a teacher if they receive offensive e-mail.*
- *Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.*
- *Use of words included in the Policy Central 'banned' list will be detected and logged.*
- *Access in school to external personal e-mail accounts may be blocked.*
- *Excessive social e-mail use can interfere with learning and may be restricted.*
- *E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.*
- *The forwarding of chain letters is not permitted.*

Published content and the school web site

- *The contact details on the Website should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.*
- *Email addresses should be published carefully, to avoid spam harvesting.*
- *The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.*
- *The Website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.*

Publishing staff and pupil's images and work

- *Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified by name.*
- *Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.*
- *Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.*
- *Pupil's work can only be published with the permission of the pupil and parents.*
- *Images of staff should not be published without consent.*

Social networking and personal publishing

- *Social networking sites and newsgroups will be blocked unless a specific use is approved.*
- *Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc.*
- *Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name, school or shopping centre.*
- *Teachers' official blogs or wikis should be password protected and run from the school website. Teachers should be advised not to run social network spaces for students on a personal basis.*
- *Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.*
- *Students should be advised not to publish specific and detailed private thoughts.*

- *Schools should be aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.*

Managing filtering

- *The school will work in partnership with the Warwickshire ICT Development Service and Becta to ensure filtering systems are as effective as possible.*
- *If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the school E-Safety coordinator.*
- *Larger schools, generally secondary, will manage the configuration of their filtering. This task requires both educational and technical experience.*
- *Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.*
- *Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP (addresses later).*

Managing emerging technologies

- *Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.*
- *Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.*
- *The school should investigate cellular wireless, infra-red and Bluetooth communication and decide a policy on phone use in school.*
- *Staff will be issued with a school phone where contact with pupils is required.*

Protecting personal data

- *Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.*

Policy Decisions

Authorising Internet access

- *The school will maintain a current record of all staff and pupils who are granted Internet access.*
- *All users must read and abide by the 'Acceptable ICT Use Policy' before using any school ICT resource.*
- *Parents will be informed that pupils will be provided with supervised Internet access (an example letter for primary schools is available).*
- *Secondary students must apply for Internet access individually by agreeing to comply with the Responsible Internet Use statement.*
- *Parents will be asked to read and acknowledge the school's 'Acceptable ICT Use Policy'.*

Assessing risks

- *In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor WCC can accept liability for the material accessed, or any consequences of Internet access.*
- *The head teacher will ensure that the e-Safety Policy is implemented and compliance with the policy monitored.*
- *The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.*
- *Methods to identify, assess and minimise risks will be reviewed regularly.*

Handling e-safety complaints

- *Complaints of Internet misuse will be dealt with by a senior member of staff*
- *Any complaint about staff misuse must be referred to the head teacher who should use the agreed WCC procedures.*
- *Pupils and parents will be informed of the complaints procedure.*
- *Parents and pupils will need to work in partnership with staff to resolve issues.*
- *Sanctions within the school discipline policy include:*
 - *interview/counselling by head of year;*
 - *informing parents or carers;*
 - *detentions;*
 - *removal of Internet or computer access for a period.*

Community use of the Internet

- *The school will liaise with local organisations to establish a common approach to e-safety.*
- *The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.*

Communications Policy

Introducing the e-safety policy to pupils

- *Pupils will be informed that Internet use will be monitored.*
- *An e-Safety training programme will be introduced to raise the awareness and importance of safe and responsible Internet use.*
- *Instruction in responsible and safe use should precede Internet access.*
- *A module on responsible Internet use will be included in the PSHE, Citizenship or ICT programmes covering both school and home use.*

Staff and the e-Safety policy

- *All staff will be given the School e-Safety Policy and its importance explained.*
- *Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.*
- *Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.*
- *Staff development in safe and responsible Internet use and on the school e-Safety Policy will be provided as required.*

Enlisting parents' support

- *Internet issues will be handled sensitively to inform parents without alarm.*
- *A partnership approach with parents will be encouraged. This could include parents' evenings with demonstrations and suggestions for safe home Internet use.*

This policy is to be read in conjunction with the Safeguarding Policy