## Acceptable Use of ICT Policies

<table>
<thead>
<tr>
<th>Version:</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version Author:</td>
<td>Till Maina</td>
</tr>
<tr>
<td>Version Ratified By:</td>
<td>Full Governing Body</td>
</tr>
<tr>
<td>Date Version Ratified:</td>
<td>September 2014</td>
</tr>
<tr>
<td>Governor’s Lead:</td>
<td>Mark Fletcher</td>
</tr>
<tr>
<td>SLT’s Lead</td>
<td>Keith Douglas</td>
</tr>
<tr>
<td>Date this version issued:</td>
<td>March 2016</td>
</tr>
<tr>
<td>Last Review Date:</td>
<td>March 2016</td>
</tr>
<tr>
<td>Next Review Date:</td>
<td>March 2019</td>
</tr>
<tr>
<td>Target Audience:</td>
<td>Governors, Staff, Parents</td>
</tr>
<tr>
<td>To Be Published On The Website</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Acceptable Use Of ICT Policies

TABLE OF CONTENTS

PART 1. OVERVIEW ................................................................................................................ 3
  INTENT ............................................................................................................................. 3
  REVIEW PROCESS ............................................................................................................ 3

POLICY 1. PUPIL USE OF THE SCHOOL COMPUTER NETWORK ................................ 4
  1. AIM ............................................................................................................................. 4
  2. PURPOSE OF THE SCHOOL COMPUTER NETWORK ................................................ 4
  3. FACILITIES FOR USE BY PUPILS .......................................................................... 4
  4. CORRECT USE OF THE NETWORK ........................................................................... 4
  5. SANCTIONS ................................................................................................................ 6
  6. APPLYING THIS POLICY .......................................................................................... 6

POLICY 2. PUPIL USE OF THE INTERNET ........................................................................ 7
  1. AIM ............................................................................................................................. 7
  2. INTERNET ACCESS FOR PUPILS ............................................................................. 7
  3. CORRECT USE OF THE INTERNET BY PUPILS ...................................................... 8
  4. SANCTIONS ................................................................................................................ 9
  5. APPLYING THIS POLICY .......................................................................................... 9

POLICY 3. STAFF USE OF THE SCHOOL COMPUTER NETWORK AND INTERNET .... 10
  1. AIM ............................................................................................................................. 10
  2. PURPOSE OF THE SCHOOL COMPUTER NETWORK FOR STAFF, ..................... 10
  3. FACILITIES OF THE SCHOOL COMPUTER NETWORK FOR USE BY STAFF .......... 10
  4. APPROPRIATE USE OF THE NETWORK AND THE INTERNET BY STAFF .......... 12
  5. SANCTIONS ................................................................................................................ 14
  6. APPLYING THIS POLICY .......................................................................................... 14

POLICY 4. PUPIL USE OF RESOURCE ROOMS .............................................................. 15
  1. AIM ............................................................................................................................. 15
  2. PURPOSE OF THE RESOURCES ROOM ................................................................... 15
  3. BOOKING PROCEDURES ......................................................................................... 15
  4. ORGANISATION OF THE ROOM .............................................................................. 16
  5. OVERCOMING COMMON DIFFICULTIES ................................................................ 16

POLICY 5. INTEGRATION OF THE AUP .......................................................................... 17
  1. AIM ............................................................................................................................. 17
  2. PROCEDURES TO MAKE THE AUP EFFECTIVE ..................................................... 17
  3. RELATIONSHIP TO OTHER SCHOOL POLICIES ..................................................... 17
  4. AREAS NOT DEALT WITH IN THE AUP ..................................................................... 19

POLICY 6. PUPIL AGREEMENT WITH THE AUP .......................................................... 20
  1. AIM ............................................................................................................................. 20
  2. CORRECT USE OF THE NETWORK .......................................................................... 20
  3. CORRECT USE OF THE INTERNET .......................................................................... 21
  4. CONSEQUENCES OF MISUSE .................................................................................... 22
  5. PUPIL SIGNATURE ..................................................................................................... 23

PART 3. APPENDICIES ........................................................................................................ 24
APPENDIX A: POSTERS TO BE DISPLAYED IN EVERY COMPUTER ROOM ............... 24
APPENDIX B: HCC ADVICE ON PROFESSIONAL RESPONSIBILITIES USING ICT ...... 26
Acceptable Use Of ICT Policies

PART 1. OVERVIEW

Intent

These policies govern the rules for use of information technology for pupils and staff. They form part of a suite of documents and policies which relate to the safeguarding responsibilities of the School.

A reference copy of this document is kept on the shared drive and it will be brought to the attention of all members of staff. An electronic copy will also be published on the School website.

Review Process

This policy will be reviewed every three years or on the introduction of new or amended relevant legislation.

John de Braux
CHAIR OF GOVERNORS

Keith Douglas
HEADTEACHER
Acceptable Use Of ICT Policies

POLICY 1. PUPIL USE OF THE SCHOOL COMPUTER NETWORK

1. **Aim**
   
   1.1. To ensure that all staff are aware of school rules concerning pupils use of the school computer network

   1.2. To ensure that all pupils use of the school computer network within school rules

2. **Purpose of the school computer network**

   2.1. The School computer network may be used by all pupils and all staff.

   2.2. The School computer network must only be used for school-related activity.

3. **Facilities for use by pupils**

   3.1. The network gives pupils access to a large number of computer programs related to their school work.

   3.2. The network enables pupils to use various devices such as printers and scanners.

   3.3. The network enables all pupils to have an area of disk space (‘their area’ = ‘My Documents’) on the central file server that no other pupil can access. In here they can save school work.

   3.4. The security of their area is achieved by use of a user name and a private password allocated by the IT Department.

   3.5. The network allows pupils to access the Internet through the Hertfordshire Grid for Learning and the schools SmoothWall filter.

   3.6. The network enables teachers to show programs in their lessons.

   3.7. The network enables teachers to take registration through Progresso.

   3.8. Anti-virus software is installed on all school PCs.

4. **Correct Use of the Network**

   Note: any point that is underlined indicates that this is a serious breach of the rules and has consequences.

   4.1. The school computer network may be used by all pupils in the school. They must only use it for educational purposes, usually directly related to their...
Acceptable Use Of ICT Policies

school work. This specifically excludes playing games when using a computer in lessons.

4.2. Pupils must not use the school network or computer equipment unless supervised.

4.3. During a lesson using computers, pupils must use only the programs that the teacher has specifically said they may use for that lesson. They must not have other programs open (even minimised). They must not use the Internet unless the teacher has specifically said that they can.

4.4. Equipment is shared. Pupils must treat all hardware (computers, peripherals, printers, cables) with care. Any attempt to damage the system (either by damaging hardware or the functioning of the software or software settings) will be treated as a serious breach of the rules.

4.5. Pupils must not remove or insert any cables or other electrical equipment into the system. It can damage the system or potentially result in electrocution.

4.6. Pupils must not attempt to log on to the system under a false user name and password. Nor should they attempt to logon with another pupil's details. Any attempt to do so is a serious breach of the rules.

4.7. Pupils must not attempt to alter the system settings or software in any way on any school computer. Any attempt to do so is a serious breach of the rules.

4.8. Pupils who feel that their password is known to others must tell their teacher who may change it for them or tell the IT Department so that it can be changed.

4.9. Pupils must save only school-related work onto the school network (includes both the network file server and all individual hard disks).

4.10. Pupils must not use a password to protect individual files. A password-protected file will be immediately deleted when found, without asking the owner’s permission. This is because anti-virus software cannot open password-protected files to find out whether they contain a virus. Therefore they are a serious risk for all users of the School Computer Network.

4.11. Pupils must only use computer programs supplied by the school. Pupils must not load any programs of their own onto the system, or download programs from the Internet. At the very least, this puts the school in danger of breaking the law by having programs on its system that it has not purchased.

4.12. Pupils must be willing to show any teacher the contents of any computer files they are carrying. All files must be school-related.

4.13. Pupils may use printers only with a teacher’s permission.
Acceptable Use Of ICT Policies

4.14. Pupils must save work to their area on the file server but must not save it to any other place on the system.

4.15. All faults must be reported to the teacher immediately and these must then be passed to IT Support using the IT Support fault reporting procedure on the VLE.

4.16. All work done by pupils using computer equipment must be appropriate. Material in a computer file is no different from material written on paper. Material which is unacceptable in school, such as abusive language, inappropriate language or images or threatening language will be treated as a very serious misuse of the system.

4.17. If a pupil is ever in doubt as to whether a particular use of a computer is appropriate or educational, then they must ask their teacher FIRST.

5. Sanctions

5.1. If a pupil misuses the system then all normal school sanctions (such as detentions) will apply. The sanctions must be applied by the teacher.

5.2. The details of any serious breach of the rules must be dealt with using the PAL form. This is a similar procedure to that used for any other serious breach of the school rules. Rules of this type are underlined in the previous section

5.3. Using the computer network is a privilege not a right. For serious breaches of the rules, the right to use the computers may be taken away, either temporarily or permanently.

6. Applying this policy

6.1. The points contained in this policy will be reinforced from time to time in ICT lessons. Other staff may wish to do this as well in their cross-curricular ICT lessons.

6.2. Staff must be familiar with the policy and be vigilant when their pupils use computers, and try to apply the principles contained in the policy as best they can.

6.3. Pupils must sign that they agree with this policy. Year 7 pupils will be sent the Acceptable User Policy as part of their Transition pack. When returned these will be held on their school record.
Acceptable Use Of ICT Policies

POLICY 2. PUPIL USE OF THE INTERNET

1. Aim

1.1. To ensure that all staff are aware of school rules concerning pupils use of the internet

1.2. To ensure that all pupils use of the internet within school falls within school rules

2. Internet access for pupils.

2.1. The Internet is to be used for school-related activity only.

2.2. All pupils have a user name and password which enable them to use the school network. This also allows them access to the Internet

2.3. School Internet access is via the Hertfordshire Grid For Learning (The Grid).

2.4. The School uses a SmoothWall filter for web sites and web pages. We use this filter for filtering out unacceptable material (such as pornographic, racist or extremist literature). No filter is 100% effective. Occasionally pupils may inadvertently gain access to pages with inappropriate content. The ICT department will explain to pupils what to do if this happens. This will be done in ICT lessons in Year 7

2.5. The school does not prohibit the use of Internet search engines.

2.6. The school provides pupils with e-mail addresses and they must use this for communicating with the school. All e-mails written or read in school are not private and must be shown to teachers if they ask.

2.7. The school cannot prevent access to chat rooms and user groups other than by the filter, but pupils must not attempt to use these internet facilities.

2.8. The school VLE may be accessed by pupils using a suitable user name and password.
Acceptable Use Of ICT Policies

3. Correct use of the Internet by pupils

Note: any point that is underlined indicates that this is a serious breach of the rules and has consequences.

3.1. The Internet must only be used for school-related activity.

3.2. Pupils must only use the Internet when specifically permitted by their teacher.

3.3. All the rules for using the school network apply to using the Internet.

3.4. If a student finds a site with material which is unacceptable, the student must report the website address to their teacher. The teacher must then pass the address on to the IT Department. This site can then be added to the filter.

3.5. Pupils must not deliberately access unacceptable material on the Internet, nor may they post such material. This is treated as a serious breach of the rules by the school, and can even lead to prosecution by the police. Unacceptable materials include pornographic, racist or extremist materials amongst others. Students should be aware that a record is kept of all the sites that each student visits.

3.6. Programs must not be downloaded from the Internet onto the school network.

3.7. E-mails written and read in school are not private and must be shown to a teacher if required. They must only contain school-related material in the same way as files stored on the network are school-related. The content must always be polite.

3.8. Material in an e-mail is no different from material written on paper. Any written material which is unacceptable in school, such as abusive language, inappropriate language or images, or threatening language will be treated as a very serious breach of the rules.

3.9. Visiting an Internet chat room is a serious breach of the rules. For the safety of pupils these must not be visited.

3.10. Pupils must not give out their personal details or anyone else’s to anyone else at all on the Internet.

3.11. Work by pupils must not be placed on the school web site unless permission has been gained from the parents of the pupil concerned.

3.12. Pupils must not download from the Internet, use or upload to the Internet any material which is copyright. They must always seek permission from the
Acceptable Use Of ICT Policies

owner, before using any material from the Internet. If in doubt, or they cannot obtain permission, they must not use the material.

3.13. Pupils must not upload photos of themselves or other pupils or teachers onto the VLE.

3.14. Pupils must not access or try to access any sites that are ordinarily blocked by the filter such as social networking sites or video upload sites.

4. Sanctions

4.1. If a pupil misuses the Internet then all normal school sanctions (such as detentions) will apply. The sanctions must be applied by the teacher.

4.2. The details of any serious breach of the rules must be dealt with using the PAL form. This is a similar procedure to that used for any other serious breach of the school rules. Rules of this type are underlined in the previous section.

4.3. Using the Internet is a privilege not a right. For serious breaches of the rules, the right to use the Internet or the school computer network may be taken away from the student, either temporarily or permanently.

5. Applying this policy

5.1. The points contained in this policy will be reinforced from time to time in ICT lessons. Other staff may wish to do this as well in their cross-curricular ICT lessons.

5.2. Staff must be familiar with the policy and be vigilant when their pupils use computers, and try to apply the principles contained in the policy as best they can.

5.3. Pupils must sign that they agree with this policy. Year 7 pupils will be sent the Acceptable User Policy as part of their Transition pack. When returned these will be held on their school record.
POLICY 3. STAFF USE OF THE SCHOOL COMPUTER NETWORK AND INTERNET

1. Aim

1.1. To ensure that staff are aware and abide by school rules for network and internet use

Note: This policy does not cover the way staff use computers when in charge of pupils. Other sections of this document cover that aspect of the system. Advice about staff use of ICT equipment outside school is included in Appendix B.

2. Purpose of the School Computer network for staff.

2.1. The School computer network and its Internet access may be used by all teaching staff and all support staff.

2.2. The school network and its Internet access is a school resource. It must only be used for school-related activity. Saving purely personal material onto the school network and undertaking purely personal Internet activity is an inappropriate use of the school system.

2.3. The network is a shared resource and staff must use the network responsibly so that the equipment and software are always available to be used when needed.

3. Facilities of the school computer network for use by staff

3.1. The network gives staff access to a large number of computer programs related to their work in school. They may use these either directly with pupils in the various Computer Rooms, or to assist in the teaching or administration of their subject.

3.2. The network enables staff to use various devices such as printers and scanners to enhance the quality of their work.

3.3. The network enables all staff to have an area of disk space (‘their area’ = ‘My Documents’) on the central file server that no-one, apart from certain staff in the IT Department can access. Departments may also have shared areas that can be accessed by all members of the department. Here they can share teaching materials and departmental documents.

3.4. The security of an area is achieved by use of a user name and a private password. These are issued to all new staff when they join. If staff have any problems with logging on, or the security of their area then they must see the IT Department immediately.
Acceptable Use Of ICT Policies

3.5. The network allows staff to access the educational resources of the Internet.

3.6. The network enables teachers to show programs to explain points in their lessons.

3.7. The network allows staff to create folders and save documents in an area called ‘Central Resources Library’. These documents can then be read or copied by pupils. Pupils are not able to save documents in this area.

3.8. Staff using computers in the school must be aware that they can access sensitive areas of the school network, which may hold student and or confidential information and that they must either “Log Off” or “lock the computer” to prevent unauthorised access to these areas, when leaving the PC unattended. Staff should also use the projectors “Freeze” function to avoid the accidental displaying of sensitive data when using a computer in a classroom.

3.9. Staff User ID’s and Passwords must be kept secure and Staff should not attempt to log on to the system under a false user name and password. Nor should they attempt to logon with another member of Staff’s details.

3.10. Internet access is gained via the Hertfordshire Grid for Learning. This access does not require a password once staff have logged on to the network.

3.11. The school automatically supplies e-mail addresses to staff and this must be used for all school correspondence.

3.12. The Computer Rooms may be booked by all members of staff for cross-curricular ICT. There is a separate section covering this.

3.13. Subject specific software may be made available on the system by the IT Department if appropriate licences have been bought by the department concerned. (See Section 3).

3.14. Class registration should be taken using the Progresso system.
Acceptable Use Of ICT Policies

4. Appropriate Use of the Network and the Internet by staff

Note: any point that is underlined indicates that this is a serious breach of the rules and has consequences.

4.1. The school computer network may be used by all teaching staff and support staff in the school. They must only use it for educational purposes, usually directly related to their work in school.

4.2. All system faults must be reported to the IT Department immediately.

4.3. Teachers who feel that their password is known to others must notify the IT Department.

4.4. The school computers are a shared resource. Please avoid monopolising a computer.

4.5. Equipment is shared. Staff must treat all hardware with care.

4.6. All hardware is owned by the school, not individual departments. All reallocation of redundant equipment between staff or departments must be done only with the IT Departments prior knowledge and approval.

4.7. Staff may save only school-related work onto the school network (includes both the network file server and all individual hard disks). They must not save non school-related work on the system.

4.8. Staff must always save work to their area on the file server, not to any other place on the system, because nowhere else is secure.

4.9. Staff must not use a password to protect individual files. Any password-protected file will be immediately deleted when found, without asking the owner’s permission. This is because anti-virus software cannot open password-protected files to discover whether they contain a virus. Therefore they are a serious risk for all users of the School Computer Network.

4.10. A file saved on a public system such as the school system is not private and the IT Department has the right to look at any file saved on the system, including staff e-mails.

4.11. Staff must only use the school e-mail supplied and must not forward on school emails to any commercially available systems.

4.12. Programs or non-school related files must not be put onto the school network.
Acceptable Use Of ICT Policies

4.13. Staff must use printers only for school work. Where the “Follow me” queue is not used, then staff have a responsibility to ensure that the IT department are aware of their ink requirements in sufficient time to enable the ink to be replenished so as not to cause ink related outages.

4.14. Staff must only use computer programs supplied by the school or their department. Staff must not load any programs of their own onto the system. At the very least, this puts the school in danger of breaking the law by having programs on its system that it has not purchased.

4.15. Subject-specific software on the system is the responsibility of individual departments. The departments must be able to produce licences for the software they have asked to be installed on the system.

4.16. The IT Department will not load software onto the system unless the correct number of licences have been purchased by the department concerned. This may be a single-user licence, for use on one computer, a class set of 30 single licences, in which case the software can be used in one room, or a site licence, in which case the software can be used on any computer in the school.

4.17. Staff must not deliberately access unacceptable material on the Internet nor may they post such material. Unacceptable materials include pornographic, racist or extremist materials amongst others. Staff should be aware that a record is kept of every site that is visited from the school system.

4.18. Staff must not access or try to access any sites such as social networking sites or video upload sites that are ordinarily blocked by the SmoothWall filter.

4.19. All work done by staff using school computer equipment must be appropriate and school-related. Material in a computer file is no different from material written on paper. Material which is unacceptable in school, such as abusive language, inappropriate language or images, or threatening language will be treated as a very serious misuse of the system.

4.20. Staff must not download, use or upload any material which is copyright from the Internet. They must always seek permission from the owner, before using any material from the Internet. If in doubt, or they cannot obtain permission, they must not use the material.

4.21. Staff must read Appendix B for advice on the use of ICT outside school.
Acceptable Use Of ICT Policies

5. Sanctions

5.1. Staff misuse of school equipment will be treated in the same way as staff misuse of other equipment.

6. Applying this policy

6.1. Staff must be familiar with this policy and apply the principles contained in the policy as best they can.
POLICY 4. PUPIL USE OF COMPUTER ROOMS

1. Aim

1.1. To ensure that teachers know the correct procedures to follow when using the room.

Note: the correct use of the school computer network by pupils is detailed in another policy and should be read by all staff intending to use the Computer Rooms.

2. Purpose of the Computer Rooms.

2.1. The Computer Rooms enables pupils and teachers to experience and benefit from ICT in any subject on the curriculum.

2.2. The Rooms cannot be used by pupils who are unsupervised. Please do not allow any unsupervised use of the room by pupils or Sixth-Formers.

2.3. Please do not send individual pupils or groups of pupils to any of the Computer Rooms (or other ICT rooms) from your lessons ‘to finish off work’. Pupils must be supervised.


3.1. The Computer Rooms can be booked by any teacher for any lesson during the week, using the booking sheet in the staff room. The room may be booked for a session after school finishes if needed.

3.2. Access to Computer Rooms is via the staff ID Key Card and on no account are the doors to be left propped open if the room is not in use. Always ensure that the room is locked at the end of any lesson.

3.3. If you wish to use the whiteboard, then you may need a pen (the pen will depend on the room being used). For Promethean boards, you will need the Promethean Pen. Smart Boards have their pens in the holder at bottom of the board.
Acceptable Use Of ICT Policies

4. Organisation of the rooms.

4.1. The teacher must use the PC nearest to the interactive whiteboard in order to use it. Pupils must not use this PC.

4.2. All malfunctioning equipment or damage must be reported to the IT Department.

4.3. The rooms can get very hot, but if you open any doors, then please remember to close it at the end of the lesson.

4.4. Please leave time for tidying the room at the end of the lesson. Ensure that the PCs are neatly arranged, the seats are under the desks and all paper is placed in the bin or recycled.

4.5. Please do a quick check that the keyboard has been placed under the monitor with the mouse placed next to the keyboard and that any headphones are placed over the monitor. Please check that no equipment such as mice has been removed during the lesson.

5. Overcoming common difficulties

5.1. Troubleshooting

5.1.1. The IT Department can be contacted via the Main Office during a lesson.

5.2. Printers and scanners

5.2.1. If the printer becomes jammed or does not print for any other reason, please tell your class to stop printing and try to clear the jam.

5.3. Pupil log on and off

5.3.1. Usernames and passwords are issued to new users by the IT Department. If any pupil has a problem logging on then you must record the pupil’s name and form and pass them to the IT Department.
POLICY 5. INTEGRATION OF THE AUP

1. Aim

1.1. To make the AUP effective and to integrate it with other existing school policies.

2. Procedures to make the AUP effective

2.1. All pupils must sign their agreement to the principles of the AUP before they can be given a user name and password. In Year 7 pupils will be sent the Acceptable User Policy as part of their Transition pack. When returned these will be held on their school record.

2.2. Gaining the signatures of pupils who join the school late will be a central responsibility.

2.3. The network rules and Internet rules will be discussed at least once in Year 7 ICT lessons and when appropriate in other ICT lessons.

2.4. The ICT department will explain to pupils what to do if they inadvertently access a site that is unacceptable. (They report it to their teacher, who passes on the address of the site to the IT Department, who adds the site address to the filter).

2.5. The details of any serious breach of the rules must be referred to the Head of ICT (for information and possibly action), Form Tutor (for information), and the Head of School for action using the PAL form. This is a similar procedure to that used for any other serious breach of the school rules.

2.6. Relevant parts of the AUP may appear on the school website.

2.7. Periodically, pupils may be selected at random and their hard disk area on the school network inspected.

2.8. The two forms ‘Responsible Use of the Network’ and ‘Responsible Use of the Internet’ will be on display by all computers that are used by pupils.

3. Relationship to other school policies.

3.1. Anti-bullying policy

3.1.1. Cyber-bullying can easily take place using computer equipment and facilities such as e-mail. It is just as serious as every other form of bullying and it must be treated as such. Refer to the Anti-bullying policy for details.
Acceptable Use Of ICT Policies

3.2. Literacy policy

3.2.1. There are powerful software tools such as spell-checkers and grammar checkers that can be effective in improving literacy. Teachers should make themselves aware of these and use them appropriately with classes.

3.2.2. Some pupils find it easier to produce written work using a computer than by hand, maybe because they have problems with handwriting or maybe because there are excellent presentation facilities in some software packages. Teachers should make themselves aware of these and use them appropriately with classes.

3.3. Equal Opportunities policy

3.3.1. All pupils are entitled to an equal opportunity to use the computer facilities within the school. Where necessary, classes are relocated to ensure that pupils with physical disabilities can have access to the facilities.

3.4. Anti-Racism policy.

3.4.1. Racism can take place using computer equipment and facilities such as e-mail. If found this is equally serious as every other form of racism and must be treated as such.

3.4.2. However, the quantity and extent of information on the Internet means that it can make a useful contribution in the teaching of different cultures and beliefs.

3.5. Numeracy policy

3.5.1. There are powerful tools such as spreadsheets that can be of use in improving numeracy. Teachers should make themselves aware of these and use them appropriately with classes.

3.6. Health and Safety

3.6.1. Safety in school is the responsibility of everyone in the school. If you have reason to suspect that any fittings or equipment in a computer room may be dangerous, then you must report this immediately in writing to the Premises manager.

3.6.2. Health and Safety matters are dealt with in more detail in the school’s Health and Safety policies.
Acceptable Use Of ICT Policies

3.7. e-safety

3.7.1. Although proper use of ICT equipment as specified in the AUP improves e-safety, the AUP is not an e-safety policy. E-safety matters are specifically dealt with in the e-safety policy itself.

4. Areas not dealt with in the AUP

4.1. Computers in the School library

4.1.1. The computers in the school library are used in a different way from other computers in the school to which pupils have access. Firstly, the Librarian must perform supervision at the same time as managing the library. Secondly the pupils are each doing different work rather than taking part in a class lesson. These combine to make control harder. However, the Viglen Remote Learning tool, should be utilised as in other Computer rooms, to assist in the monitoring of internet activity. In all other respects the same basic computer usage procedures should be applied.
Acceptable Use Of ICT Policies

POLICY 6. PUPIL AGREEMENT WITH THE AUP

1. Aim

1.1. To make clear to pupils what they may do and not do when using the School Computer Network and Internet

2. Correct Use of the Network

2.1. The school computer network may be used by all pupils in the school. They must only use it for educational purposes, usually directly related to their school work. This specifically excludes playing games.

2.2. Pupils must not use the school network or computer equipment unless a teacher is supervising.

2.3. During a lesson using computers, pupils must only use the programs that the teacher has specifically said they may use for that lesson. They must not have other programs open (even minimised). They must not use the Internet unless the teacher has specifically said that they can.

2.4. Equipment is shared. Pupils must treat all hardware (computers, peripherals, printers, cables) with care. Any attempt to damage the system (either by damaging hardware or the functioning of the software or software settings) will be treated as a serious breach of the rules.

2.5. Pupils must not remove or insert any cables or other electrical equipment into the system. It can damage the system or potentially result in electrocution.

2.6. Pupils must not attempt to log on to the system under a false user name and password. Nor should they attempt to logon with another pupil's details. Any attempt to do so is a serious breach of the rules. Every pupil has access to the network and there is never justification for trying to gain access to another person's area. A pupil’s area may contain examination work and this must be protected.

2.7. Pupils must not attempt to alter the system settings or software in any way on any school computer. Any attempt to do so is a serious breach of the rules.

2.8. Pupils who feel that their password is known to others must tell their teacher who will either change it or will contact the IT Department so that it can be changed.

2.9. Pupils must save only school-related work onto the school network.
Acceptable Use Of ICT Policies

2.10. Pupils must not use a password to protect individual files. A password-protected file will be immediately deleted when found, without asking the owner’s permission.

2.11. Pupils must only use computer programs supplied by the school. Pupils must not load any programs of their own onto the system, or download programs from the Internet. At the very least, this puts the school in danger of breaking the law by having programs on its system that it has not purchased.

2.12. Pupils must be willing to show any teacher the contents of any computer files they are carrying. All files on a removable storage device must be school-related.

2.13. Pupils must check all data (on files) brought into school for viruses before it is used on school computers. Anti-virus software is installed on all school PCs. Viruses cause damage to files.

2.14. Pupils must only use printers with a teacher’s permission.

2.15. Pupils must always save work to their area on the file server.

2.16. All faults must be reported to the teacher immediately.

2.17. All work done by pupils using computer equipment must be appropriate. Material in a computer file is no different from material written on paper. Material which is unacceptable in school, such as abusive language, inappropriate language or images, or threatening language will be treated as a very serious misuse of the system.

2.18. If a pupil is ever in doubt as to whether a particular use of a computer is appropriate or educational, then they must ask their teacher FIRST.

3. Correct use of the Internet

3.1. The Internet must only be used for school-related activity.

3.2. Pupils must only use the Internet when specifically permitted by their teacher.

3.3. All the rules for using the school network apply to using the Internet.

3.4. If a student finds a site with material which is unacceptable, the student must report the website address to their teacher.

3.5. Deliberately accessing unacceptable material on the Internet is treated as a serious breach of the rules by the school, and can even lead to prosecution by
Acceptable Use Of ICT Policies

the police. Students should be aware that a record is kept of all the sites that each student visits.

3.6. Programs must not be downloaded from the Internet onto the school network.

3.7. The school provides pupils with e-mail addresses and they must use this for communicating with the school. All e-mails written or read in school are not private and must be shown to teachers if they ask. They must only contain school-related material in the same way as files stored on the network are school-related.

3.8. Material in an e-mail is no different from material written on paper. Any written material which is unacceptable in school, such as abusive language, inappropriate language or images, or threatening language will be treated as a very serious breach of the rules.

3.9. Pupils must not download, use or upload any material which is copyright. They must always seek permission from the owner, before using any material from the Internet. If in doubt, or they cannot obtain permission, they must not use the material.

3.10. Pupils must never give out the personal details of themselves or anyone else to anyone else at all on the Internet.

3.11. Work by pupils will not be placed on the school web site unless permission has been gained from the parents of the pupil concerned.

3.12. Pupils must not access or try to access any sites such as social networking sites or video upload sites that are ordinarily blocked by the filter.

3.13. Pupils must not upload photos of themselves or other pupils or teachers onto the VLE.

4. Consequences of Misuse

4.1. If a pupil misuses the School Computer Network or the Internet, then all normal school sanctions (such as detentions) will apply.

4.2. The details of any serious breach of the rules will be reported to either the Head of ICT, a Head of School, or the IT Services Manager, in the same way as any serious breach of the rules is dealt with generally.

4.3. Using the School Computer Network or the Internet is a privilege not a right. For serious breaches of the rules, the right to use the computers may be taken away from the pupil, either temporarily or permanently - even if the student needs to use the school network for their examination work.
Acceptable Use Of ICT Policies

4.4. All teachers and the IT Department have the right to look at any file in any pupil’s area on the school network, or any file that is being used by a pupil at the school, including files on removable storage devices and e-mails.

4.5. Periodically, pupils may be selected at random and their hard disk area on the school network inspected.

5. Pupil Signature

5.1. Pupils must sign that they agree with the principles in this policy before they can use the School computer Network or the Internet from the school’s connection.

5.2. Signatures will be collected for new year 7 pupils, after they have been sent the Acceptable User Policy as part of their Transition pack. When returned these will be held on their school record.
Responsible Network Use

*Computers in the school have a large number of excellent programs that you should use whenever possible to help with school-related activities.*

1. A teacher must be supervising
2. The computers are only for educational use (no games)
3. Treat all computer equipment with care
4. Do not touch any of the electrical connections
5. Do not log on with anyone else’s user name and password
6. Use only the programs supplied by the school. Never load your own programs onto the system
7. Only school-related work is to be saved on the network
8. Permission must be sought to use an electronic storage device and you must show a teacher the contents of the files on your electronic storage device if asked
9. Only print with the teacher’s permission
10. Do not eat or drink in computer rooms, or while using a computer.

*Ask a teacher if you are unsure*
Responsible Internet Use

_The school encourages pupils to use the Internet, because it contains a wealth of valuable educational material. Remember though, that in school, the Internet must only be used for school-related activity._

1. Do not download programs from the Internet
2. Do not give out your personal details
3. Do not join mailing lists
4. Do not visit web-sites unless they are educational
5. Do not try to access sites containing pornographic, racist or extremist materials
6. Do not play games on the computers
7. Do not visit chat-rooms, social networking sites or user groups
8. E-mails written and read at school are not private and must be shown to a teacher if the teacher asks to see it
9. E-mails must always be polite
10. Do not use material from the Internet as if it was your own – always acknowledge the author

_Ask a teacher if you are unsure_
Acceptable Use Of ICT Policies

Remember: a record is kept of every web site visited by every student

APPENDIX B: HCC ADVICE ON PROFESSIONAL RESPONSIBILITIES USING ICT

Advice sheet from Hertfordshire County Council, Standards & School Effectiveness, eSafety Team V1 October 2010 in conjunction with NAHT, ASCL, NUT, NASUWT, ATL Unison

"Professional responsibility when using any form of ICT, including the Internet, in school and outside school

For your own protection we advise that you:

- Ensure all electronic communication with pupils, parents, carers, staff and others is compatible with your professional role and in line with school policies.

- Do not talk about your professional role in any capacity when using social media such as Facebook and YouTube.

- Do not put online any text, image, sound or video that could upset or offend any member of the whole school community or be incompatible with your professional role.

- Use school ICT systems and resources for all school business. This includes your school email address, school mobile phone and school video camera.

- Do not give out your own personal details, such as mobile phone number, personal e-mail address or social network details to pupils, parents, carers and others.

- Do not disclose any passwords and ensure that personal data (such as data held on MIS software) is kept secure and used appropriately.

- Only take images of pupils and / or staff for professional purposes, in accordance with school policy and with the knowledge of SLT on school owned equipment.

- Do not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

- Ensure that your online activity, both in school and outside school, will not bring your organisation or professional role into disrepute.

- You have a duty to report any eSafety incident which may impact on you, your professionalism or your organisation."