ALL SAINTS
ACADEMY PLYMOUTH

E-LEARNING, E-SAFETY & ICT FOR LEARNING POLICY

Author of Policy
Mal Nash
Vice Principal

Date adopted by Governors/Academy
December 2014

____
Signed on behalf of Governing Body

Date reviewed
December 2014

All Saints Church of England Academy, Plymouth aims to be an inspirational community of learning, which will transform the life chances of the students and make a positive contribution to the well-being of the local community and the wider world. The Academy is rooted in Christian values including truth, justice, forgiveness, generosity and respect. The Academy aims to provide outstanding educational opportunities and experiences which will enable all students, regardless of ability and background, to bring out the best in themselves, and to make a difference for good in the world.

The Academy believes that education is about the development of the whole person, and in educating each student will endeavour to:

- sharpen the mind
- enrich the imagination
- strengthen the body
- nourish the spirit
- encourage the will to do good
- open the heart to others

This policy and the associated procedures are based on these principles, aims and beliefs.

Introduction

This policy is made up of three key issues related to e-learning, e-safety and best practice ensuring that the use of computers by staff and students are maximised and used within the guidelines of the law.

Purpose

The statutory curriculum expects students to learn how to locate, retrieve and exchange information using IT. In delivering the curriculum, teachers need to plan for and make use of communications technology, for example, web-based resources and email. Access to life-long learning and employment requires computer and communications use and students need to develop life skills in their use, ICT is a significant tool to enhance teaching and learning at All Saints Academy, Plymouth.

Procedure

Definition and Forms of e-learning

E-learning may be defined as any form of instruction where computer technology, and other technologies, are used and applied to facilitate learning.
E-Learning provision may be either:

- Web-supported
- Web-dependent
- Fully online

Web supported

This form of e-learning is used to provide students with easy access to basic information such as teacher notes, practice exam questions, module handbooks, PowerPoint presentations, etc. It runs in parallel with face-to-face teaching, which continues as the more prominent mode of delivery. Online participation would not usually be assessed either, though students may receive feedback from teachers on homework/coursework progress etc.

Web-dependent

This form of e-learning contains all the elements of the above with online participation by students being required, and may be assessed. Online content would therefore be more substantial than notes or PowerPoint presentations and will have been developed using a range of e-learning activities [e-tivities] and exercises. An example of this could be collaborative learning, e.g. peer, group or learning sets could be used and teacher feedback could be considerable.

Fully Online

Students interact exclusively online and generally they would not attend face-to-face classes. Interaction between teachers and fellow students would be conducted within a VLE [Virtual Learning Environment]. Such courses/modules would be supported by a strongly tested and developed e-learning infrastructure.

In developing a working framework for e-learning within the Academy, each of the above is regarded, for the purposes of this policy, as a separate and therefore planned developmental stage in policy implementation. At the time of writing this policy it is expected that for most students, face-to-face teaching will be their most familiar instructional experience.

E-safety

E-safety depends on effective practice at a number of different levels:

- Responsible IT use by all staff and students; encouraged by education and made explicit through published policies
- Sound implementation of e-safety policy in both administration and curriculum, including secure Academy network design and use
- Safe and secure broadband
- National Education Network standards and specifications

Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The Academy has a duty to provide students with quality Internet access as part of their learning experience
- Internet use is a part of the statutory curriculum and a necessary tool for staff and students

Internet use will enhance learning

- The Academy Internet access will be designed expressly for student use and will include filtering appropriate to the age of students
- Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

Students will be taught how to evaluate Internet content

- The Academy will ensure that the use of Internet derived materials by staff and by students complies with copyright law
- Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

Information system security

- Academy IT systems capacity and security will be reviewed regularly
- Virus protection will be installed and updated regularly
- Security strategies will be discussed with the local authority

Email

- Students may only use approved email accounts on the Academy system
- Students must immediately tell a teacher if they receive offensive email
- Students must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission
- Email sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on Academy headed paper
- The forwarding of chain letters is not permitted

Published content and the Academy website

- The contact details on the website should be the Academy address, email and telephone number. Staff or students' personal information will not be published
- The Principal [or nominee] will take overall editorial responsibility and ensure that content is accurate and appropriate

Publishing student's images and work

- Photographs that include students will be selected carefully and will not enable individual students to be clearly identified.
- Students' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the Academy website.
- Work can only be published with the permission of the student and parents.

Social networking and personal publishing

- The Academy may block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Students will be advised never to give out personal details of any kind which may identify them or their location.
- Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and know how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.

Managing filtering

- The Academy will work in partnership with the South West Grid for Learning to ensure systems to protect students are reviewed and improved.
- If staff or students discover an unsuitable site, it must be reported to the Network Manager.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing video-conferencing

- Students should ask permission from the supervising teacher before making or answering a video conference call.
- Video conferencing will be appropriately supervised for the students' age group.

Managing emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the Academy is allowed.

Protecting personal data

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

Authorising IT and Internet access

All staff must read and sign both the 'IT Acceptable Use Policy' and 'Internet Acceptable Usage Policy' forms before using any Academy IT resources.

The Academy will maintain a current record of all staff and students who are granted access to Academy IT systems.

- All students must read and sign both the 'IT Acceptable Use Policy' and 'Internet Acceptability Usage Policy' forms before using any Academy IT resources.
- Parents will be asked to sign and return the forms.

Assessing risks

The Academy will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on an Academy computer. The Academy cannot accept liability for the material accessed, or any consequences of Internet access. The Academy should audit IT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

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 Principal.
- Complaints of a child protection nature must be dealt with in accordance with Academy child protection procedures.
- Students and parents will be informed of the complaints procedure.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Introducing the e-safety policy to students

- E-safety rules will be posted in all networked rooms.
- Students will be informed that network and Internet use will be monitored.

Staff and the e-safety policy

All staff will be given the Academy 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 IT use will be supervised by senior management and have clear procedures for reporting issues.

Enlisting parents' support

Parents' attention will be drawn to the Academy e-safety policy in newsletters, the Academy prospectus and on the Academy website.

COMPUTER SECURITY

1. Physical Equipment Security

- Where possible, computer equipment will be sited so as to reduce the risk of unauthorised access and damage.
- The details of all computer equipment will be recorded in the official inventory record together with relevant serial numbers.
- Computer hardware will be appropriately security marked.
- A record will be kept of any computer equipment taken off site. The removal of equipment from the Academy's premises must be authorised by the Principal.

2. Backup Procedures

- All data held on the Academy's computer system will be backed every evening the Academy is open. Personal data held on individual computers will NOT be backed up.
- Backups are rotated every two weeks and will be clearly labelled.
- A year-end backup of financial data will be taken and retained using separate disks each year.
- The officer responsible for backup procedures for the System Network is the Network Manager.

3. Virus Detection

- All computers will have virus detection software installed within their start-up procedures. The Network Manager updates the software regularly.
- Any disks of uncertain origin must be scanned for viruses before use.
- The use of unlicenced software is prohibited.
- Any perceived virus attach should be immediately reported to the Network Manager.
- The officer responsible for virus detection procedures is the Network Manager.

4. Software Controls

- All software is maintained by the Academy and must be properly owned by the Academy. Software may only be used in accordance with the licence agreement. Personally owned software WILL be removed.
- The Network Manager will hold all licences and system disks so that they are aware of all the software installed in Academy. The system disks are stored in the locked IT room cupboard.
- The Network Manager will keep an inventory of all software maintained on the Academy's computers, together with relevant serial numbers.
- Access to software will be restricted to authorised staff.
- The Network Manager is the only person who may issue passwords and amend access levels.
- Users of the Academy's computer system will be issued with individual passwords.
- It should be ensured that passwords are kept confidential.
- Staff should LOCK the computer system before leaving any PCs unattended.
- When staff leave, their accounts will be disabled immediately by the Systems Manager.
- Any suspected breach of security will be immediately reported to the Principal.
- The officer responsible for software control is the Network Manager.

5. Legal Obligations

- All staff should be made aware of the requirements and their responsibilities in relation to the following legal statutes:

  1984 Data Protection Act
  1986 Copyright, Design and Patents Act
  1990 Computer Misuse Act.

6. Acquisition, Maintenance and Disposal of Hardware

- The Principal has overall responsibility for the acquisition, maintenance and disposal of equipment.
- ALL IT related software and equipment purchases MUST go through the Vice Principal to be able to compare 'best prices' and 'best value'.
- Official orders will be used for purchases.
- The write off and disposal of equipment should be authorised by the Governing Body and the Principal.
- Acquisition and disposal of equipment must be in accordance with the Financial Regulations for Academies.

7. User Training

- Users should receive appropriate training in the correct use of the Academy's IT facilities including use of software packages and security arrangement.

8. Disaster Recovery

- There will be adequate arrangements in place for disaster recovery including emergency procedures, manual fallback plans and resumption of procedures.
- The officer responsible for disaster recovery is the Network Manager as the backup of the Academy network includes the server, financial systems and student's administration.

9. Internet Access

- There will be adequate procedures in place to ensure that access to the Internet is appropriate for the person accessing it and the necessary blocks and security measures are in place to prevent misuse.
- The officer responsible for maintaining the Internet access is the Network Manager.

10. Key Personnel

- Network Manager – responsible for maintaining and securing the Academy's main network and server systems. In their absence, support will be provided by his department.
- Finance Director – responsibility for the management of the Academy's financial software package. In their absence, the day-to-day operation of the department would be continued by the finance assistant.

Resources

IT Acceptable Use Policy- Staff

The Academy has provided IT facilities for use by staff, offering access to a vast amount of information for use in studies and offering great potential to support the curriculum.
The IT facilities are provided and maintained for the benefit of the entire Academy community, and you are encouraged to use and enjoy these resources, and help to ensure they remain available to all.

Equipment

- Always get permission from the Network Manager before installing, attempting to install or storing programs of any type on the computers. Evidence of licence will be required.
- All maintenance should be carried out by IT support staff.
- Always check files brought in on removable media [such as floppy disks, CDs, flash drives etc.] with antivirus software and only use them if they are found to be clean of viruses.
- Protect the computers from spillages by eating or drinking well away from the IT equipment or IT suites.

Security and Privacy

- Protect your work by keeping your password to yourself; do not use someone else's logon name or password without the specific permission of the Principal.
- Always be wary about revealing your home address, telephone number, Academy name, or picture to people you meet on the Internet.
- Other computer users should be respected and should not be harassed, harmed, offended or insulted.
- To protect yourself and the systems, you should respect the security on the computers; attempting to bypass or alter the settings may put you or your work at risk.
- Your files and communications may be monitored to ensure that you are using the system responsibly.

Internet

See the Internet Acceptable Usage Policy

Email

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is as anti-social on the Internet as it is on the street
- Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer
- If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, always report such messages to your line manager. The sending of an email containing content likely to be unsuitable for Academies is strictly forbidden
- Spam:
    - Be careful with your email address on the Internet.
    - You may receive spam if you publish your email address on a website, in a posting to a news group or in an online form [e.g. to send an electronic greeting card].
    - Never reply to a spam message, no matter how annoying! By replying, you let the sender know that your email address exists and then you are likely to receive more spam.
    - Never unsubscribe using links in spam email. This lets the sender know your email address is active – you are likely to receive even more spam.
    - Never open attachments! Files attached to spam email often contain viruses. Delete the email immediately.
- The @asap.org.uk account provided by IT support should be used for all communications with staff, students, parents and other agencies.
- Webmail:
    - Webmail should not be used for the communications listed in the point above.

Physical security

- Main Academy students in an IT room should be supervised by a member of Academy staff at all times. Main Academy students should not be sent around the Academy to look for a vacant IT suite during lessons or to see if there are spare computers in an IT suite when a lesson is taking place. Students may be sent to an IT room if a prior arrangement has been made with the teacher using that room. The teacher in the IT room will then be responsible for supervising them. Alternatively, students may be sent to the library.
- In order to maximise access for post-16 students, they will be allowed access to a vacant IT suite during lesson time. However to gain this access the students will have to find a key holder. The key holder must ensure that the room is locked immediately that the room becomes vacant again. There must also be at least two post-16 students in a room at any time.
- Outside of lesson times [this includes before school, break times, lunch time and after school] no student should have any access without direct supervision from a member of staff [i.e. the supervisor is in the room all the time that students are there].
- Doors to IT suites should be kept locked at all times when vacant.

Images of students

- Ensure that parental permission has been gained for the use of any student's image.
- Avoid publishing the first and last name of a student with a photograph of them. This reduces the risk of inappropriate, unsolicited attention from people outside Academy. An easy rule to remember is:

  - If the student is named, avoid using the photograph
  - If a photograph is used, avoid naming the student

- Consider using group photos rather than photos of individual students.
- Only record images of students in suitable dress to reduce the risk of inappropriate use.
- Images should be stored in a designated central area on the Academy network, not in an individual teacher's user area. They should be deleted from any other temporary storage media at the time of uploading on to the network. This should be done within a reasonable time after the recording of the images.
- Ensure that the image file is appropriately named. Do not use students' names in image files or on ALT tags if published on the web.
- The images will be deleted once their period of use has expired. The teacher responsible for recording the images must ensure that they are deleted. If the teacher has left the Academy then their line manager assumes this responsibility.

Personal equipment

- Personal mobile phones and other portable devices such as portable digital assistants [PDAs] should not be used to communicate with students.
- Staff must not give out personal mobile phone numbers to students.
- If it is necessary to record students' mobile phone numbers for an Academy trip or other event, the record of the numbers should be destroyed after the trip or event.

- In the case of members of the public, including parents, visiting the Academy site, they may only record images [still or video] of a student where specific permission has been granted by that student's parent or legal guardian.

Licences

- All Software, Music, Images, Videos MUST have a licence that covers use in the Academy.
- A copy of this must be given to Network Manager.
- No ITunes or other music, files, images can be attached to the Academy network at any time unless a licence can be produced.

Monitoring

- The Academy reserves the right to monitor electronically all activity on its network and any device attached to it. This includes computers, laptops, flash drives, MP3s etc whether they belong to the Academy or not.
- This can be visually or via software and will be used as evidence if required in any disciplinary procedures that may come from misuse.

Please read this document carefully. If you violate these provisions you will be subject to disciplinary action. Additional action may be taken by the Academy. Where appropriate, police may be involved or other legal action taken.

Name: ____

Date: ________________________________

Signed: ____

Internet Acceptable Usage Policy – Staff

The purpose of this policy is to ensure that users of the All Saints Academy Plymouth [ASAP] network understand the way in which the Internet is to be used. The policy aims to ensure that the Internet is used effectively for its intended purpose, without infringing legal requirements or creating unnecessary risk. Users should read this policy alongside the IT Acceptable Use Policy.

Scope

The policy applies to all users and administrators of the ASAP network services and/or infrastructure. On evidence provided by ASAP, an employee may be disciplined. At the same time, if a user's conduct and/or action[s] are illegal, the user may become personally liable in some circumstances.

Policy statement

ASAP encourages users to make effective use of the Internet. Such use should always be lawful and appropriate. It should not compromise ASAP's information and computer systems nor have the potential to damage ASAP's reputation.

Use of Internet facilities

ASAP expects all users to use the Internet responsibly and strictly according to the following conditions: For the purposes of this document, Internet usage means any connection to the Internet via web browsing, external email or news groups.

Users shall not:

Visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- pornography [including child pornography]
- promoting discrimination of any kind
- promoting racial or religious hatred
- promoting illegal acts
- any other information which may be offensive to other users in the Academy community.

ASAP acknowledges that in certain planned curricular activities, access to otherwise deemed inappropriate sites may be beneficial for educational use [for example investigating racial issues]. Any such access should be pre-planned and recorded so that it can be justified if required. This should be carried out in consultation with the appropriate line manager. Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material will be reported to the police:

- Images of child abuse [images of children, apparently under 16 years old] involved in sexual activity or posed to be sexually provocative
- Adult material that potentially breaches the Obscene Publications Act in the UK
- Criminally racist material in the UK.

If inappropriate material is accessed accidentally, users should immediately report this to the ASAP Network Manager so that this can be taken into account in monitoring.

Users shall not:

- Use the ASAP facilities for running a private business
- Enter into any personal transaction that involves ASAP
- Visit sites that might be defamatory or incur liability on the part of ASAP or adversely impact on the image of ASAP
- Upload, download, or otherwise transmit [make, produce or distribute] commercial software or any copyrighted materials belonging to third parties outside of ASAP, or to ASAP itself
- Reveal or publicise confidential or proprietary information, which includes but is not limited to:

    - financial information
    - personal information
    - databases and the information contained therein
    - computer/network access codes
    - business relationships

- Intentionally interfere with the normal operation of the Internet connection, including the propagation of computer viruses and sustained high volume network traffic [sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion] that substantially hinders others in their use of the Internet
- Use the Internet for soliciting, representing personal opinions or revealing confidential information or in any other way that could reasonably be considered inappropriate

Monitoring
ASAP will monitor and audit the use of the Internet to see whether users are complying with the policy. Any potential misuse identified by ASAP will be reported to the Network Manager and/or other relevant person.
Please read this document carefully. If you violate these provisions you will be subject to disciplinary action. Additional action may be taken by the Academy. Where appropriate, police may be involved or other legal action taken.

Name: ____

Date: ________________________________

Signed: ____

IT Acceptable Use Policy - Student

The Academy has provided IT facilities for your use, offering access to a vast amount of information for use in studies and offering great potential to support your learning.

The IT facilities are provided and maintained for the benefit of the entire Academy community, and you are encouraged to use and enjoy these resources, and help to ensure they remain available to all.

You are responsible for good behaviour with the resources and on the Internet just as you are in a classroom or an Academy corridor.

Equipment

- Never attempt to install or store programs of any type on the computers.
- All maintenance should be carried out by IT support staff.
- Always check files brought in on removable media [such as floppy disks, CDs, flash drives etc.] with antivirus software and only use them if they are found to be clean of viruses.
- Do not eat or drink in the vicinity of the IT equipment or IT suites.
- Turn off any equipment when you have finished using it unless you are instructed otherwise by a member of staff

Security and Privacy

- Protect your work by keeping your password to yourself; never use someone else's logon name or password.
- If you find a computer that another user has forgotten to log off from then inform a member of staff.
- Other computer users should be respected and should not be harassed, harmed, offended or insulted.
- To protect yourself and the systems, you should respect the security on the computers; attempting to bypass or alter the settings is unacceptable behaviour.
- Your files and communications will be monitored to ensure that you are using the system responsibly.

Internet

See the Internet Acceptable Usage Policy

Email

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is as anti-social on the Internet as it is on the street.
- Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer.
- If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, always report such messages to a member of staff. The sending

of an email containing content likely to be unsuitable for young people or Academies is strictly forbidden.

- Spam:
  - Be careful with your email address on the Internet.
  - You may receive spam if you publish your email address on a website, in a posting to a news group or in an online form [e.g. to send an electronic greeting card].
  - Never reply to a spam message, no matter how annoying! By replying, you let the sender know that your email address exists and then you are likely to receive more spam.
  - Never unsubscribe using links in spam email. This lets the sender know your email address is active – you are likely to receive even more spam
  - Never open attachments! Files attached to spam email often contain viruses. Delete the email immediately.
- The @asap.org.uk account provided by IT support should be used for all communications with Academy staff and for communicating with other students for Academy work purposes.
- Webmail such as hotmail should not be used at all in the Academy.
- The use of email for bullying will be investigated and dealt with in accordance with the Academy anti-bullying policy.

Physical security

- Main Academy students in an IT room should be supervised by a member of Academy staff at all times. You should not be sent around the Academy to look for a vacant IT suite during lessons or to see if there are spare computers in an IT suite when a lesson is taking place. You may be sent to an IT room if a prior arrangement has been made with the teacher using that room by your teacher. The teacher in the IT room will then be responsible for supervising you and you must follow their instructions. Alternatively, you may be sent to the library.
- Outside of lesson times [this includes before school, break times, lunch time and after school] no student should have any access without direct supervision from a member of staff [i.e. the supervisor is in the room all the time that students are there].
- Doors to IT rooms should be kept locked at all times when vacant. Inform a member of staff if you know that an IT room has been left open.

Images of students

- You should always ask another student or a member of staff for permission before recording their image. If they do not give you permission then you must respect their decision.
- Consider using group photos rather than photos of individual students.
- Any images of you held by the Academy will be deleted once their period of use has expired, or you have left the Academy.

Personal equipment

- Personal mobile phones and other portable devices such as portable digital assistants [PDAs] and MP3 players should only be used with your teacher's permission on Academy equipment.

  - Use of personal mobile digital equipment for bullying will be investigated and dealt with in accordance with the Academy anti-bullying policy.

- Staff must not give out their personal mobile phone numbers to you.
- Staff may ask you for your mobile phone number during an Academy trip or other event. You do not have to give it if you do not wish to. If you do give your mobile phone number to a member of staff, the record of your number will be destroyed after the trip or event.

Licences

- All Software, Music, Images, Videos MUST have a licence that covers use in the Academy.
- A copy of this must be given to Network Manager.
- No iTunes or other music, files, images can be attached to the Academy network at any time unless a licence can be produced.

Monitoring

- The Academy reserves the right to monitor electronically all activity on its network and any device attached to it. This includes computers, laptops, flash drives, MP3s etc whether they belong to the Academy or not.
- This can be visually or via software and will be used as evidence IF required in any disciplinary procedures that may come from misuse.

Please read this document carefully. If you violate these provisions you will be subject to disciplinary action. Where appropriate, the police may be involved.

Name: ____ Student

Date: _____________________________

Signed: ____ Student

Signed: ____ Parent

Internet Acceptable Usage Policy - Student

The purpose of this policy is to ensure that users of the All Saints Academy Plymouth [ASAP] network understand the way in which the Internet is to be used. The policy aims to ensure that the Internet is used effectively for its intended purpose, without infringing legal requirements or creating unnecessary risk. Users should read this policy alongside the IT Acceptable Use Policy.

Policy statement

ASAP encourages users to make effective use of the Internet. Such use should always be lawful and appropriate. It should not compromise ASAP's information and computer systems nor have the potential to damage ASAP's reputation.

Please read this policy carefully as you will be deemed to be aware of its contents.

Use of Internet facilities

ASAP expects all users to use the Internet responsibly and strictly according to the following conditions: For the purposes of this document, Internet usage means any connection to the Internet via Web browsing, external email or news groups.

Users shall not:

Visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- pornography [including child pornography]
- promoting discrimination of any kind
- promoting racial or religious hatred
- promoting illegal acts
- any other information which may be offensive to other members of the Academy community.

If inappropriate material is accessed accidentally, you should immediately report this to your teacher so that this can be taken into account in monitoring.

Incidents which appear to involve deliberate access to Websites, newsgroups and online groups that contain the following illegal material will be reported to the police:

- images of child abuse [images of children, apparently under 16 years old] involved in sexual activity or posed to be sexually provocative
- adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist material in the UK.

If you accidentally access illegal material, you should immediately tell a teacher. Do not touch the computer.

Users shall not:

- Use the ASAP facilities for running a private business
- Enter into any personal transaction that involves ASAP or the Local Authority in any way
- Visit sites that might be defamatory or incur liability on the part of ASAP or the Local Authority or adversely impact on the image of ASAP
- Upload, download, or otherwise transmit [make, produce or distribute] software or any copyrighted materials belonging to third parties outside of ASAP, or to ASAP itself
- Reveal or publicise confidential or proprietary information, which includes but is not limited to:

  - financial information
  - personal information
  - databases and the information contained therein
  - computer/network access codes
  - business relationships

- Intentionally interfere with the normal operation of the Internet connection, including the spreading of computer viruses and sustained high volume network traffic [sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion such as playing network games] that substantially hinders others in their use of the Internet
- Use the Internet for soliciting, representing personal opinions or revealing confidential information or in any other way that could reasonably be considered inappropriate

Monitoring

ASAP will monitor and audit the use of the Internet to see whether users are complying with the policy. Any potential misuse identified by ASAP will be reported to the Network Manager and/or other relevant person.

Please read this document carefully. If you violate these provisions you will be subject to disciplinary action. Additional action may be taken by the Academy. Where appropriate, police may be involved or other legal action taken.

Name: ____ Student

Date: _______________________________

Signed: ____ Student