Staniland Academy

ICT Acceptable Use Policy (AUP)

Monitoring Responsibility	CEO
Next Review Date	June 2019
Approval Body	Trust Leadership
Date Ratified	
Chair of Committee Signature	

Contents

1. ICT curriculum policy

2. A statement of basic conventions, use of internet and web 2.0 technologies.

3. Computer security and data protection

4. Information regarding network records and logs.

5. Guidelines for staff and learners and information on what constitutes a violation of the acceptable use policy.

6. Academy policies and sanctions for violations of the agreed AUP.

7. Information regarding possession of unsuitable material and computer misuse.

8. Commitment by users to respect academy procedures:

    a. Head of Academy's internet permission letter.

    b. User commitment letter.

    c. Parent / carer permission letter.

1. ICT curriculum policy

Vision

Staniland Academy is committed to developing innovative uses of ICT in order to harness its immense power to the benefit of learners, staff and members of the wider community. Our learners will be equipped with the necessary knowledge and skills empowering them to become autonomous and discerning users of twenty-first century technologies. ICT will be used as an educational tool to enhance learning within the academy and reform communication within the connected learning community.

We will raise learner expectations and achievements and make them aware of the implications of ICT in all aspects of society. As teachers we must ensure that ICT is a core of excellence.

Rationale

In order to create the skill base for the new millennium we must make the most of technological change. Technology has revolutionised the way we work and live and is now set to transform education and learning. The broad application of ICT is already a fundamental aspect of our society. We live in a world of pervasive information technology where computers act and take decisions on our behalf infinitely more quickly than we can ourselves. The use of ICT is now a common tool in the home, in industry and in commerce. Individuals cannot be effective in tomorrow's world if they are trained in yesterday's skills. Nor should teachers be denied the tools that other professionals take for granted.

Confidence in the use of ICT and discrimination in the selection of its applications will be essential requirements of adult life. Teaching and learning through ICT not only offers the chance to become proficient in the skills needed in the world of work, it enhances and enriches learning and the curriculum, raising standards and motivating learners.

Aims

We aim to enable our learners to become confident, competent, independent and discerning users of ICT. To this end we aim to:

- Make ICT an integral part of the curriculum.
- Enhance learning and teaching across all faculties using ICT.
- Provide opportunities for learners to become autonomous, effective and discerning users of ICT.
- Provide opportunities and support to develop staff skills and competence.
- Provide support and training for our partner primary academies.
- Develop, maintain and stimulate learners' curiosity, interest and enjoyment in ICT
- Allow learners to develop transferable skills and informed opinions about their ICT skills and be able to support them with reasoned argument.
- Encourage all subject teachers to see how ICT and their subject expertise link together to their mutual benefit.

- Support all staff in their need to develop confidence and strategies in using ICT within their teaching. To recognise that INSET and support for staff are vital if learners are to progress in ICT capability.

Objectives

Staniland Academy views ICT as a vital tool in all learners' education, in all areas of the curriculum. We seek to achieve the following objectives:

- Each learner leaving the academy should be ICT literate, having had good opportunities to use and develop individual skills in every faculty area.
- Learners should be capable of using basic packages such as word-processing, spreadsheets, databases, graphics and desktop publishing packages to a high standard and be able to transfer the skills between packages, faculties and tasks.
- Learners should be capable of solving problems using logical thinking and provide solutions using computing concepts such as programming, flow charts or algorithms.
- Each learner should be capable of saving and retrieving work from all software packages and be able to adapt skills already learned to new situations.
- Each learner should be able to use computers to complete work, assess work, monitor work and communicate with others safely.
- All learners should have opportunities to use computers for measurement and for the control of other devices (including data logging)
- All learners should evaluate the impact of ICT on their lives.

At Staniland Academy, ICT is creative as well as functional. We aim to support and enhance the whole curriculum, emphasising, when appropriate, the place of the new technologies in our society. Teachers will aim to teach in a meaningful context whilst providing opportunities for learners to use their skills creatively. Teachers will strive to ensure that the quality of learning and teaching is excellent.

Staffing

Support and guidance in all matters related to curriculum development, staff development, assessment and teaching and learning strategies in ICT will be provided to staff by the Trust's ICT Partners, supported by the Trust Data Protection Officer (DPO).

The ICT Technicians will provide technical support for both academic and management systems.

Responsibilities

Directors:

- To approve all ICT curriculum and financial plans.

Chief Executive Officer:

- To oversee all ICT provision.
- To monitor finance, hardware and software provision.
- To agree and implement spending plans.

Head of Academy

- To manage the budget
- To lead and encourage whole-academy curriculum use of ICT
- To monitor all ICT curriculum initiatives and projects
- To agree staff development needs with the INSET Co-ordinator

SLT:

- Responsible for the day-to-day co-ordination of the ICT curriculum.
- To monitor and evaluate progress in ICT.
- To support cross-curricular projects.
- To monitor all ICT curriculum initiatives, projects and assessment within curriculum.
- To support cross-curricular ICT projects.
- To co-ordinate assessment.

Network Manager

- To implement all network, hardware and software requirements.
- To maintain inventories of all ICT hardware and software.
- To implement backup and security of all data.
- To perform day to day maintenance and support of ICT systems

ICT Support Staff

- To perform day to day maintenance and support of ICT systems
- To assist learners in classroom use of ICT

All Teaching Staff

- To deliver and assess all planned projects in the classroom.
- To be responsible for raising awareness of their own ICT development needs.

Hardware and Software
The academy has standardised hardware and software around the PC platform running the Windows operating system. All future purchasing decisions will be based around the principle of ensuring compatibility with existing systems. It is recognised that ICT is a quick changing resource and these priorities are deemed to be flexible.

The academy deploys class management and web filtering systems to monitor the use of the network across the academy and to ensure the safety of staff and learners.

Monitoring
The Head of Academy and the Network Manager will liaise with the Chief Executive Officer regarding any developments within the academy's ICT provision.

Evaluation and Review
The ICT Development Plan will be reviewed annually by the Trust Special Interest Group for ICT. The Chief Executive Officer will evaluate progress and make budget decisions for the following years.

2. A statement of basic conventions, use of internet and web 2.0 technologies.

What is the internet?
The internet is a world-wide collection of computer networks, e.g. a network of networks, capable of mass communication and resource sharing. In most cases, each computer linked to this network is also linked locally to a number of other computers, in a local network. This network of networks makes it possible for someone using a local computer network to access information on any of the other computers in the world wide network.

What is the World Wide Web?
The World Wide Web is a global interactive multimedia system that is run over the Internet to make the appearance of information more attractive and the process of finding information easy and efficient.

Most web pages contain text, colours, pictures, sound, video and interactive media elements e.g. Flash or JavaScript. These pages, collectively, make up what is known as the World Wide Web. Most of these pages include information on the location of other pages on the World Wide Web, and it is possible to follow up links between pages with similar or related content. Moving from one page to another, is called browsing, or surfing. Many of these web pages contain information that is useful in an educational context for both teaching and learning.

What is Electronic Mail? (Email)
Electronic mail is the process of sending messages and files electronically using computer networks. A message consists of text content, an author address, one or more recipient addresses and possibly a file attachment. Each user has a unique e-mail address e.g. anybody@anywhere.com that link to current email systems. Email systems that operate over a network are based on a store-and-forward model in which computer server systems accept, forward, deliver and store messages on behalf of users who will

view their email the next time they log on. Rarely is email transmitted directly from one user's device to another's.

Internet e-mail addresses are usually provided along with the academy's connection to the internet and provision has been made for every learner to have their own individual e-mail address. This allows each learner to send messages and to receive messages from those people whose addresses they have previously listed or a school based contact list. This prevents them from receiving unsolicited e-mail and reduces the external threat of spam and viruses etc.

What are News Groups and Blogs?
News groups are a collection of messages written for public domain rather than individuals. Each group of messages is focused on a particular subject or theme. Individuals can read these messages and also post replies. Replies are kept in the public domain (available to everyone). In this way it is possible to track a multi-way conversation about an important issue of the day. At present there are millions of different topics available for discussion, from specialist science research, to support groups for asthma, to fans of James Bond movies.

What are web 2.0 technologies?
Web 2.0 technologies are a second generation of web development and design technologies that facilitates communication, secure information sharing, interoperability, and collaboration on the World Wide Web. These technologies include but are not limited to:

Wikis
A wiki is a webpage or set of web pages that can be easily edited by anyone who is allowed access.) An example of this type of technology is Wikipedia.

Social Networking
A social networking website is an online community of people who share interests and activities, or who are interested in exploring the interests and activities of others. Social networking websites provide web based services for users to interact, such as e-mail and instant messaging. An example of this type of technology is Facebook.

Tagging and Bookmarking
Social bookmarking is a method used to store, organize, search, and manage bookmarks of web pages. These bookmarks are usually in the form of tags that collectively become known as social tagging and can include text, pictures and videos. An example of this type of technology is Myspace.

Multimedia Sharing
A multimedia sharing website allows individuals to upload multimedia e.g. pictures and video clips to an internet website. The host will then store the pictures or video on its server, and show the individual different types of code

to allow other people to view the multimedia object. An example of this type of technology is YouTube.

Audio Blogging and Podcasting
A podcast is a series of audio or video digital-media files distributed over the Internet by syndicated download. Syndicated downloads rely on special software applications known as podcatchers (e.g. iTunes.) These podcatchers automatically identify and retrieve new files when they are made available.

An audio blog is a blog (see news groups and blogs) that mainly publishes audio files (music or podcasting) and makes them available for download.

RSS
An RSS feed is a method of publishing information that is continually updated e.g. blog entries, news headlines, audio, and video to a webpage or a desktop application. RSS feeds are read by a RSS reader and can benefit readers who want to subscribe to updates from favourite websites or link feeds from many sites to one place.

What are the dangers of the Internet referred to in the media?
There is some material on the Internet that is offensive to most people, examples include pornography, racist and fascist material, and this can be accessed by children if using the internet unsupervised. The main educational providers try to 'filter' known offensive locations of material of this kind, but there is too much for this filtering to be very effective, and the locations of this material change frequently. The only way to block access to this kind of material is to have a restricted range of pages available, in which case many of the advantages of the global and dynamic nature of the internet may be lost. It is a feature of the Internet that the information available is free. Increasing restrictions will undoubtedly lead to systems of charging for access to specific material, in addition to the other costs described. An alternative system is to educate learners and encourage an acceptable use policy and partnership between home and academy in dealing with the less savoury side of internet use.

How can I get more information?
There are many magazines in newsagents that cater for beginners-advanced use of the Internet. For specific questions please contact the academy's Head of Academy.

3. Staff Security and Data Protection

This guidance should be read in conjunction with the BWAF Data Protection Policy May 2018.

Staff Accounts

All staff will be provided with an individual account for accessing the academy computer system, this will include a username and password. Each staff account will be tailored to the level of access required by each staff member, and is for individual use only. As such, passwords must not be disclosed.

Unattended Computers

When leaving a computer unattended, staff must ensure they have either logged off, or locked the computer to prevent unauthorised access to their account.

Sensitive Data

Staff must not store any sensitive or personal information on any laptop or portable storage system (such as a USB memory stick, portable hard disk, or personal computer) unless that storage system is encrypted and approved for such use by the academy. If in any doubt you must see the Network Manager.

Staff must not transmit any sensitive or personal information via email without the data being encrypted by a method approved by the academy. When publishing or transmitting non-sensitive material outside of the academy, staff must take steps to protect the identity of the individual.

If a staff member wishes to use a personal computer at home for work purposes, they must ensure that any academy-related sensitive or personal information is secured to prohibit access by any non-member of staff.

Backup

Staff are advised to make regular backups of all data kept on any storage system other than the network storage drives or your 'My Documents' folder. This includes USB memory sticks (even those owned or issued by the academy) or a personal computer.

Storage

Staff members must ensure that items of portable computer equipment (such as laptops, digital cameras, or portable projectors) are securely stored in a locked room or cupboard when left unattended.

4. Information regarding network records and logs

The academy retains computer system log files to:

- Help fine tune the academy's computing systems.
- Monitor system performance and use.
- Track and identify security breaches.
- Identify areas of inappropriate usage.
- Provide information for proactive cost monitoring tools.
- Provide audit evidence if required.

It should be noted that any personal information kept is in line with the Trust's Data Protection and Record Management policies.

The following represents the current list of log files that the academy records and stores. This list may change as technology changes and other requirements are identified.

Windows Based Computers

- Authentication records.
- Application usage logs. (Only as required).
- Applications installed
- Patch update via the local event log.
- Antivirus software detection and update logs.
- Disk usage and space allocation logs.
- Email logs including to/from/date/time for Imap attached clients.
- Web mail access login with machine name and authentication process.
- A copy of all emails received is kept for archival purposes. Access to these is controlled by privacy laws.
- Web history (local machine)
- System update logs
- History of system reboots.

Learner Record System (SRS)

- Transactional logs

Network

- IP network usage logs
- Date and time logs for Webportal changes.
- Print Logs including time/size/cost/file name/user name

5. Guidelines for staff and learners and information on what constitutes a violation of the AUP

This guidance should be read in conjunction with the Staff Code of Conduct, the Social Media Usage Guidance and the BWAF Data Protection Policy May 2018.

Use of the academy computer network and Internet is a privilege, not a right. A user who violates this agreement shall, at a minimum, have his or her access to the network and the internet terminated and is subject to disciplinary action by the academy leadership. If necessary the academy will refer cases of computer misuse to the police or other relevant authorities.

All members of staff have a responsibility to use the academy's computer system in a professional, lawful, and ethical manner. Deliberate abuse of the academy's computer system may result in disciplinary action, including termination of contract and civil and/or criminal liability.

The academy recognises that the distinction between computer use at work and computer use at home is increasingly blurred, with many of us now using our own computers for work. While the academy neither wishes nor intends to dictate how you use your own computer, staff should consider that the spirit of this policy applies whenever you are undertaking an activity that stems from your employment with the academy. As such the use of trust and individual ICT platforms, including social media, shall not be used to promote services or business operations of trust staff or other related parties.

Unacceptable use of the Network may include:

A. Illegal Activities

- Sending or displaying offensive messages or pictures, to include "sexting" (the distribution of sexually explicit material).
- Accessing, uploading, downloading or distributing pornographic material
- Violating copyright laws.
- Accessing or downloading any material in violation of the law
- Cracking (unauthorized attempt to discover a computer password).
- Hacking (unauthorized attempt to bypass security).
- Impersonation (the act of pretending to be someone else by setting up a false profile, or stealing someone's password with a view to posting false material that will endanger them, cause them distress or cause them to be falsely accused).

B. Inappropriate Language & Harassment in electronic communication

- Using vulgar or obscene language in any electronic communication.
- Harassing, insulting, defaming, denigrating, or attacking others.
- Spamming other users by sending unsolicited junk email (including chain letters).
- Commenting on 'blogs' or without permission of the supervising teacher.
- Cyberstalking (cyber threats or blackmail using digital resources).
- Outing (deliberately sharing someone's personal or sensitive information).

C. Endangering Personal Safety

- Revealing personal contact information (home address, telephone number, personal details, id numbers, etc.) to other individuals over the internet.
- Arranging to meet people contacted over the internet without approval.

D. Breaching System Security

- Intentionally spreading viruses, worms, chain letters, or Trojans.
- Vandalising computers or peripheral equipment, computer systems or computer networks.
- Altering, moving or deleting the files belonging to others.

- Using another's password, or providing your password to another person.
- Unauthorized attempt to access the network, including use of the network on someone else's login.
- Attempting to access the network without providing assigned user name and password at the log-on screen.
- Using any internet 'service' that attempts to 'spoof','mask' or 'hide' its identity from the academy network security e.g. 'proxy' sites or proxy anonymisers.

E. Invading Privacy

- Trespassing in another's folders, work or files.
- Reposting a message that was sent to you privately, without permission of the original sender;

F. Misuse of Limited Resources

- Use of the network for commercial purposes.

G. Misuse of technologies (including Web 2.0 technologies)

- Learners accessing instant messaging or social networking websites during academy hours on an academy device unless specifically under the guidance of teaching/associate staff for educational purposes.
- Staff accessing instant messaging or social networking websites during academy directed time on an academy device unless it is directly linked to work of the academy
- Signing into any web based service, requiring personal details in exchange for a user name and password for further access not explicitly authorised by the teacher.
- Posting unauthorised academy or LA related video or audio to public spaces, e.g. YouTube, Google Video, Facebook, MySpace etc, either as a 'member' of the service or anonymously.
- Altering, deleting or moving any digital materials produced on any 'social space' without permission of the owner.
- Commenting on other people's work appearing on any space within public domain without permission of the teacher.
- Publishing any copyrighted materials provided to learners in class to public domain. (Teacher and academy generated media is subject to copyright.)
- Posting, downloading or plagiarising any work posted to social spaces as reference materials.
- Digital Information supplied by staff to learners in the course of their studies must not be published in any form to the public domain. Materials are subject to copyright and remain the property of the academy at all times.
- Accessing games and personal entertainment sites not directly related to the area of study at time of access.
- Staff should not allow learners access to personal social networking pages and should not "befriend" learners or parents/carers (allowing as friends in a social networking context) e.g. on Facebook.

- Staff are strongly advised to think carefully about befriending ex-learners. Ex-learners may still have siblings or other contacts at the academy.
- Staff should not post information on social networking sites about themselves or academy-related matters that they wouldn't want colleagues, learners or parents/carers to see.
- Staff should always protect social networking pages using the security settings on their account and are advised to ensure that personal information is not accessible to the public via default settings. Staff are advised to set social networking information visibility to 'Friends only'.
- When communicating with learners or parents/carers staff should not use a personal e-mail address or their own mobile phone.
- Staff are referred to the **Abuse of Social Media Policy** for further information and guidance.
- Learners are referred to the **Sanctions for Abuse of Social Media** and the **Abuse of Social Media Policy** for further information and guidance

6. Academy policies and sanctions for violations of the Acceptable Use Policy

Learner access to the Internet

The academy encourages use by learners of the rich information resources available on the Internet, together with the development of appropriate skills to analyse and evaluate such resources. These skills will be fundamental in the society our learners will be entering.

On-line services significantly alter the information landscape for schools by opening classrooms to a broader array of resources. In the past, teaching and library materials could usually be carefully chosen. All such materials would be chosen to be consistent with national policies, supporting and enriching the curriculum while taking into account the varied teaching needs, learning styles, abilities and developmental levels of the learners. Internet access, because it may lead to any publicly available site in the world, will open classrooms to electronic information resources which have not been selected by teachers as appropriate for use by learners.

Electronic information research skills are now fundamental to the preparation of citizens and future employees during this information rich age. The academy expects that staff will begin to investigate possibilities and blend use of such information as appropriate within the curriculum and that staff will provide guidance and instruction to learners in the appropriate use of such resources. Staff will consult the Head of Academy for advice on content, training and appropriate teaching levels consistent with the academy's ICT programme of study.

Access to on-line resources will enable learners to explore thousands of libraries, databases, and bulletin boards while exchanging messages with people throughout the world. The academy believes that the benefits to learners from access to information resources and increased opportunities for collaboration exceed the disadvantages. But ultimately, parents and guardians of children and young people are responsible for setting and conveying the standards that their children should follow when using media and information sources. To that end, the academy supports and respects each family's right to decide whether or not to apply for independent access. The academy's Head of

Academy will prepare appropriate procedures for implementing this policy and for reviewing and evaluating its effect on teaching and learning.

Resource Development

In order to match electronic resources as closely as possible to the national and academy curriculum, teachers need to review and evaluate resources in order to offer "home pages" and menus of materials that are appropriate to the age range and ability of the group being taught. SLT will provide appropriate guidance to learners as they make use of telecommunications and electronic information resources to conduct research and other studies. All learners will be informed by staff of their rights and responsibilities as users, before their first use, either as an individual user or as a member of a class or group.

As much as possible, the academy's chosen information provider has organised information resources in ways that point learners to those that have been reviewed and evaluated prior to use. While learners may be able to move beyond those resources to others that have not been evaluated by staff, they shall be provided with guidelines and lists of resources particularly suited to the learning objectives. Learners may pursue electronic research independent of staff supervision only if they have been granted parental permission and have submitted all required forms. Permission is not transferable and may not be shared.

Academy Rules

Infractions of the acceptable use policy will be dealt with according to the academy discipline policy. (See Guidelines and information on what constitutes a violation of the AUP.) e.g. cyber bullying imposes the same sanctions as face to face bullying (linked to the academy's anti-bullying policy.)

The academy has developed a set of guidelines for internet use by learners. These rules will be made available to all learners, and kept under constant review. All members of staff are responsible for explaining the rules and their implications. All members of staff need to be aware of possible misuses of on-line access and their responsibilities towards learners.

Learner guidelines for Internet use

Learners are responsible for good behaviour on the Internet just as they are in a classroom or an academy corridor. General academy rules apply. The Internet is provided for learners to conduct research and communicate with others. Parent/carer permission is required. Remember that access is a privilege, not a right and that access requires responsibility.

Individual users of the Internet are responsible for their behaviour and communications over the network. It is presumed that users will comply with academy standards and will honour the agreements they have signed. Staff may review learner files and communications to insure that they are using the system responsibly. Users should not expect that files stored on the servers are private. The network manager will, as a matter

of course, review user directories and delete any unnecessary material that is considered to be taking up unacceptable amounts of disc space.

During academy time, teachers will guide learners toward appropriate materials. Outside of academy time, families are responsible for such guidance as they must also exercise with other information sources such as television, telephones, movies, radio and other potentially offensive media.

For detailed information regarding internet use refer to section 3 (Guidelines for staff and learners and information on what constitutes a violation of the AUP.)

7. Information regarding possession of unsuitable material and computer misuse.

Any user who is found in possession of unsuitable material or found responsible for computer misuse shall, at a minimum, have his or her access to the network and Internet terminated either temporarily or permanently depending on the violation and is subject to disciplinary action by the academy leadership. If necessary the academy will refer cases of computer misuse to the police or other relevant authorities. In a case of referral the 1990 computer misuse act can be applied:

The Computer misuse act 1990 covers 3 main topics:

- Unauthorised access to computer material
- Unauthorised access with intent to commit or facilitate commission of further offences
- Unauthorised modification of computer material

Unauthorised access to computer material

A person is guilty of an offence if:

1. He/she causes a computer to perform any function with intent to secure access to any program or data held in any computer;
2. The access he/she intends to secure is unauthorised.
3. He/she knows at the time when he/she causes the computer to perform the function that that is the case.

A person guilty of an offence under this section shall be liable on summary conviction to imprisonment for a term not exceeding six months or to a fine not exceeding level 5 on the standard scale or to both.

<u>Unauthorised access with intent to commit or facilitate commission of further offences</u>

A person is guilty of an offence if:

He/she commits an offence under section 1 above ("the unauthorised access offence") with intent:
(a) to commit an offence to which this section applies; or
(b) to facilitate the commission of such an offence (whether by himself or by any other person);

A person guilty of an offence under this section shall be liable on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both; and on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

<u>Unauthorised modification of computer material</u>

A person is guilty of an offence if:

He/she commits an act which causes an unauthorised modification of the contents of any computer; and at the time when he does the act he has the requisite intent and the requisite knowledge.

He/she does any act to cause a modification of the contents of any computer and by so doing:

(a) to impair the operation of any computer;

(b) to prevent or hinder access to any program or data held in any computer;

(c) to impair the operation of any such program or the reliability of such data.

A person guilty of an offence under this section shall be liable on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both; and on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

8. Commitment by users to respect academy procedures:

Internet Permission Letter

Dear Parent/ Carer,

Internet Permission Form

As part of the academy's ICT programme we offer learners supervised access to the Internet, the global network of computers you will have read about and seen on television. Before being allowed to use the Internet, all learners must obtain parental permission and both they and you must sign and return the enclosed form as evidence of your approval and their acceptance of the academy rules on this matter.

Access to the Internet will enable learners to explore thousands of libraries, databases, and bulletin boards while exchanging messages with learners from our partner schools abroad. Families should be warned that some material accessible via the Internet may contain items that are illegal, defamatory, inaccurate or potentially offensive to some people.

Whilst our aim for Internet use is to further educational goals and objectives, learners may find ways to access other materials as well, even though we are using up-to-date filtering processes. We believe that the benefits to learners from access to the Internet, in the form of information resources and opportunities for collaboration, exceed any disadvantages. But ultimately, parents and carers of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. To that end, the academy supports and respects each family's right to decide whether or not to apply for access.

During academy time, teachers will guide learners toward appropriate materials. Outside of academy time, families bear the same responsibility for such guidance as they exercise with information sources such as television, telephones, movies, radio and other potentially offensive media.

We would be grateful if you would complete the permission form which follows.

Yours sincerely

Rachel Hydes
Head of Academy

Parent / Carer / Learner Internet Permission Form

Learner Name:

As an academy user of the Internet, I agree to comply with the academy rules on its use. I will use the network in a responsible way and observe all the restrictions explained to me by the academy.

I will respect copyright laws and not plagiarise others' work.

For educational purposes I will keep personal details private and not make them available to others using the internet.

I will not attempt to access unsuitable material.

I will allow members of staff to check external storage for viruses and unsuitable material.

If I fail to follow the acceptable use policy then I accept the consequences relevant to my actions and accept that I may lose the right to network and internet access.

Learner Signature _____   Date: ___/___/___

Parent/Carer

As the parent/carer of the learner signing above, I grant permission for my son or daughter to use electronic mail and the Internet. I understand that learners will be held accountable for their own actions. I also understand that some materials on the Internet may be objectionable and I accept responsibility for setting standards for my daughter or son to follow when selecting, sharing and exploring information and media.

Parent/Carer Signature   _____ Date ___/___/___

Name of Learner   _____ Date ___/___/___