Hans Price Academy
E-Safety Policy

Contents

Introduction

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The Academy wishes to promote staff and students' positive and use of these new technologies safely. This policy sets out the range of issues and the Academy's approach to them.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.
The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. This e-safety policy helps to ensure safe and appropriate use. The development and implementation of such a strategy involves all the stakeholders in a child's education from the Principal and Councillors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students themselves.
The use of these exciting and innovative tools in Academy and at home has been shown to raise educational standards and promote student achievement.
However, the use of these new technologies can put young people at risk within and outside the Academy. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and earning of the young person
- Many of these risks reflect situations in the off-line world and we recognise that this e-safety policy is used in conjunction with other Academy policies (eg behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

Scope

This policy applies to all members of the Academy community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of Academy ICT systems, both in and out of the Academy, and to personal ICT devices used on the Academy site, or off site on Academy business.

The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the Academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to

incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of Academy, but is linked to membership of the Academy.

The Academy will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of Academy.

Roles and Responsibilities

Academy Councillors

Councillors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

Principal and Senior Leaders

- The Principal is responsible for ensuring the safety (including e-safety) of members of the Academy community, though the day to day responsibility for e-safety will be delegated to Vice Principal with responsibility for Every Child Matters.
- The Principal and Vice Principals are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The Vice Principal with responsibility for Child Protection takes lead responsibility for e-safety, liaising with the Head of eLearning as necessary.

Head of eLearning

The Head of eLearning is responsible for ensuring that the ICT managed service:-

- provides an infrastructure that is secure and is not open to misuse or malicious attack
- provides systems that meet the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policies
- only allows access to the Academy's networks through a properly enforced password protection policy, in which passwords are regularly changed
- provides appropriate filtering of web content and user communications

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:-

- they have an up to date awareness of e-safety matters and of the current Academy e-safety policy and practices
- they have read, understood and signed the Academy Staff Acceptable Use Policy
- they report any suspected misuse or problem to the Year Achievement Co-ordinator for investigation and action
- digital communications with students should be on a professional level
- e-safety issues are embedded in appropriate aspects of the curriculum and other Academy activities
- students understand and follow the Academy e-safety and acceptable use policy
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra-curricular and extended Academy activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current Academy policies with regard to these devices

Child Protection Officer

The Child Protection Officer is trained in e-safety issues and is aware of the potential for serious child protection issues to arise from:-

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

Students

- Are responsible for using the Academy ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to Academy systems.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand Academy policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand Academy policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of the Academy and realise that the Academy's E-Safety Policy covers their actions out of the Academy.

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The Academy will help parents understand these issues through parents' evenings, newsletters, letters, leaflets and the Academy website. Parents and carers will be responsible for:

- Endorsing (by signature) the Student Acceptable Use Policy
- Accessing the Academy's online systems in accordance with the relevant Academy Acceptable Use Policy.

Policy Statements

Educational and Training

Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the Academy's e-safety provision. Children and young people need the help and support of the Academy to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:-

- A planned e-safety programme should be provided as part of both ICT, PBL and PHSE lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in Academy and outside the Academy
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Students should be taught in appropriate lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information

Parents and carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of their children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.

The Academy will therefore seek to provide information and awareness to parents and carers through:-

- Letters, newsletters, web site and email communications
- Parents evenings

Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the Academy e-safety policy and ICT Standards

Academy Councillors

Councillors should take part in e-safety training and awareness sessions, with particular importance for those who are members of any group involved in ICT, e-safety, health and safety or child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Governors Association/SWGfL or other relevant organisation.
- Participation in Academy training/information sessions for staff or parents

Technical – Infrastructure, Equipment, Filtering and Monitoring

The IT systems in the Academy are maintained by the Cabot Learning Federation ICT Services Team, comprising on-site and remote staff. In addition, our ICT Supplier is implementing new systems as the Academy develops. The Academy will do its utmost to ensure that the technical requirements to support e-safety are in place, specifically by ensuring:-

- Academy ICT systems will be managed in ways that ensure that the Academy meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy
- The Academy access the web through a double filtered system - firstly through a service provided by the managed service provider and subsequently by South West Grid for Learning
- There will be regular reviews and audits of the safety and security of Academy ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to Academy ICT systems
- All users will be provided with a username and password. Users will ensure that their password is secure by choosing a suitably complex word, and changing it at least every term.
- Requests from staff for sites to be removed from the filtered list will be considered by the Team Leader, Information and Communications
- Actual and potential e-safety incidents are reported to the Year Achievement Co-ordinators who may in turn consult with the Team Leader, Information and Communications
- Provision exists for temporary access by "guests" (eg trainee teachers, visitors) onto the Academy system.
- Staff are permitted to install programmes on some Academy devices where this does not interfere with the proper operation of that device or the Academy network
- All users may use removable media (eg USB flash drives, CDs and DVDs) on Academy devices
- The Academy infrastructure and individual workstations are protected by up to date virus software
- Personal data can not be sent over the internet or taken off the Academy site unless safely encrypted or otherwise secured. (see Data Security Policy)

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

Safety

- Students should learn the risks associated with using the internet, strategies for minimising those risks and dealing with incidents that occur on-line

Information literacy

- Students should learn to be critically aware of the content they access on-line and be guided to validate the accuracy of information
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

Use of Digital and Video Images – Photographic and Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The Academy will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites
- Staff are allowed to take video and images to support educational aims, but must follow Academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on Academy equipment; the personal equipment of staff should not be used for such purposes
- Care should be taken when taking video and images that students are appropriately dressed and are not participating in activities that might bring the individuals or the Academy into disrepute
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students or staff will be selected carefully and will comply with good practice guidance on the use of such images
- Students' full names will not be used on an Academy website or blog, particularly in association with photographs
- At the time of admission, parents or carers are given the opportunity to refuse to allow photographs of their children to be published on the Academy website and elsewhere. A list of students who have refused this permission is kept available

Data Protection and Security

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection

All users ensure that they:

- Become more security aware, raise any security concerns, and report incidents
- When working online on Academy systems or business, they use devices with appropriate security updates and security software (eg anti-virus and anti-spyware).
- Report spam or phishing emails
- Use secure passwords on all devices that can access personal data, changed at least annually
- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse

- Use personal data only on secure password protected computers and other devices such as smarthones, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data
- Transfer data using encryption and secure password protected devices
- Wherever possible, access data remotely and securely instead of taking it off-site
- When personal data is stored on any portable computer system, USB flash drive or any other removable media:
    - the data must be encrypted and password protected
    - the device must be password protected
    - the device must offer approved virus and malware checking software
    - the data must be securely deleted from the device, once it has been transferred or its use is complete

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following activities are not forbidden, provided that such activities do not interfere or cause harm or offence to others. Although an activity is permitted under this policy, staff may choose to limit some or all of these activities with the group under their leadership at their discretion:-

- Mobile phones and other handheld digital devices (PDA, smartphone, mp3 recorder, PSP etc.) may be brought to the Academy
- Use of handheld digital devices in lessons
- Use of handheld digital devices in social time
- Taking photos on mobile phones or other digital devices
- Use of personal email addresses in Academy, or on Academy network
- Use of Academy email for personal emails
- Use of chat rooms/facilities
- Use of instant messaging
- Use of social networking sites
- Use of blog

When using communication technologies the Academy considers the following as good practice:

- The official Academy email service may be regarded as safe and secure and is monitored
- Users need to be aware that Academy email communications may be monitored
- Users should immediately report, to a member of staff, the receipt of any communication that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such communication
- Any digital communication between staff and students or parents/carers (email, chat, VLE etc) must be professional in tone and content and should take place on Academy systems
- Students should learn about email safety issues, such as the risks attached to the use of personal details
- They should also learn strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material
- Personal information should not be posted on the Academy website and only official email addresses should be used to identify members of staff

Unsuitable and Inappropriate Activities

The Academy believes that the activities referred to in the following section would be inappropriate in an Academy context and that users, as defined below, should not engage in these activities in the Academy or outside the Academy when using Academy equipment or systems. This policy restricts certain internet usage as follows:

Expressly forbidden

- Users shall not visit web sites, run software, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:
    - child sexual abuse images
    - promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation
    - adult material that potentially breaches the Obscene Publications Act in the UK
    - criminally racist material in UK
    - pornography
    - promotion of any kind of discrimination
    - promotion of racial or religious hatred
    - threatening behaviour, including promotion of physical violence or mental harm
    - any other information which may be offensive to users or breaches the integrity of the ethos of the Academy or brings the Academy into disrepute
- Using Academy systems to run a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the Academy
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer/network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high volume network traffic (eg downloading/uploading files, streaming) that causes network congestion and hinders others in their use of the internet
- Playing games rated above the age of the user in the UK
- On-line gambling
- Spoofing, phishing, spamming or engaging in any other activities online that may cause confusion, disquiet, disruption or harm to members of the Academy, the wider community, or the public, or to their computing devices
- any other illegal activity related to computer or internet use

Inappropriate use

The Academy also considers the following activities to be inappropriate and to constitute misuse and perpetrators can expect to be sanctioned (see next section):-

- Excessive or inappropriate personal use of the internet/social networking sites/instant messaging/personal email
- Harmful downloading or uploading of files
- Allowing others to access Academy network by sharing username and passwords or attempting to access or accessing the Academy network, using another person's account
- Careless use of personal data eg holding or transferring data in an insecure manner
- Deliberate actions to breach data protection or network security rules

- Corrupting or destroying the data of other users or causing deliberate damage to hardware or software
- Sending a communication that is regarded as offensive, harassment or of a bullying nature
- Communications between staff and students on personal systems
- Actions which could compromise a staff member's professional standing
- Actions which could bring the Academy into disrepute or breach the integrity of the ethos of the Academy
- Using proxy sites or other means to subvert the Academy's filtering system
- Deliberately accessing or trying to access offensive or pornographic material, or running software that contains such material
- Breaching copyright or licensing regulations
  As a guide, any material that would be considered by public broadcasters as unsuitable to be shown on early evening terrestrial television is considered inappropriate in the Academy

Responding to Incidents of Misuse

It is hoped that all members of the Academy community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:
If any apparent or actual misuse appears to involve illegal activity ie.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

the usual action will be taken and the incident will be reported to the police. Steps should be taken to preserve evidence where possible.
If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the SWGfL "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress" should be followed. This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer.
It is more likely that the Academy will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the Academy community are aware that incidents have been dealt with. It is intended that incidents of misuse such as those detailed in the previous section will be dealt with through the normal behaviour/disciplinary procedures for both staff and students.

Standards of Acceptable Use

Student ICT Standards

I understand that I must use Academy ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I accept that the Academy uses secure online systems for the storage and communication of my personal information, such as Gmail and SIMS.

For my own personal safety:

- I understand that the Academy will monitor my use of the ICT systems, email and other digital communications
- I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username and password
- I will be aware of "stranger danger", when I am communicating on-line
- I will not disclose or share personal information about myself or others when on-line
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line

Equal rights to technology as a shared resource:-

- I understand that the Academy ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work
- I will not use the Academy ICT systems for gambling, shopping, running a business, unless I have permission of a member of staff to do so
- I will not store files unnecessarily, and shall ensure that I keep my file storage requirements to a minimum. I shall not store files that are not connected with my learning on the Academy systems.

Respect for others:-

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions
- I will not take or distribute images or other recordings of anyone without their permission.

Maintaining security and a purposeful learning environment:-

- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials
- I will immediately report any damage or faults involving equipment or software, however this may have happened

- Although many kinds of technology are permitted within the Academy, I recognise that in some situations, the use of technology is inappropriate and distracting. I shall respect staff's instructions on the use of technology.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of the Academy:

- *I may bring my own handheld digital devices (mobile 'phone, PDA, smartphone, mp3 recorder, PSP etc.) to the Academy, but this will be entirely at my own risk*. I will not use these devices to make recordings of people in the Academy without their permission. I must not let the use of these technologies detract from my learning. I will stop using these devices if requested by a member of staff.
- I understand that the Academy also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of the Academy and where they involve my membership of the Academy community (examples would be cyber-bullying, use of images or personal information)
- I understand that if I fail to comply with these Standards, I will be subject to disciplinary action. This may include loss of access to the Academy network/internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

These standards apply whenever:-

- I use the Academy ICT systems and equipment (both in and out of the Academy)
- I use my own equipment in the Academy (when allowed) e.g. mobile phones, netbooks, cameras etc.
- I use my own equipment out of the Academy in a way that is related to me being a member of this Academy e.g. communicating with other members of the Academy, accessing Academy email, VLE, website etc.

Staff ICT Standards

I understand that I must use Academy ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems, the data held on them, and other users. I accept that the Academy uses secure online systems for the storage and communication of personal information, such as Edmodo, Gmail and Progresso. I recognise the value of the use of ICT for enhancing learning and will ensure that students receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- *I understand that the Academy may monitor my use of the ICT systems, email and other digital communications.* This includes the location of mobile devices.
- *I understand that the standards set out here also apply to use of Academy ICT systems (e.g. laptops, email, realsmart, other online sites etc) out of the Academy*
- *I understand that the Academy ICT systems are primarily intended for educational use and that any personal or recreational use I make of the equipment or systems must not interfere with their educational purpose, for myself or others*
- *I will keep all devices, systems and accounts secure with physical and password protection. I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I will change my password at least annually,* and if I have access to particularly sensitive information, I shall change it at least three times a year.
- *I will prevent unauthorised access to devices and accounts by logging out, or locking my computer before leaving it*
- *I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person*

Professional communications and actions

- *I will not access, copy, remove or otherwise alter any other user's files, without their permission*
- *I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions*
- *I will ensure that when I take or publish recordings of others (images, video, audio) I will do so with their permission.* Parents have the opportunity to refuse permission for recordings of their children to be used; I shall check this list before making use of any recordings. I shall ensure that any recordings I make fulfill an educational purpose and are appropriate. I will only use Academy equipment to record, store and retrieve such recordings. I shall only store such recordings on Academy accounts. Where these images are published (e.g. on the Academy website) full names will only be used with permission
- I will only communicate with students and parents/carers using official Academy systems. Any such communication will be professional in tone and manner. I will not befriend, follow or otherwise link to students or parents/carers using on-line networking accounts other than those operated by the Academy.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- I shall abide by the Academy Email Protocol when sending emails

Safe and secure access to technologies and smooth running of the Academy:

- *I may bring my own handheld digital devices (mobile 'phone, PDA, smartphone, mp3 recorder, PSP etc.) to the Academy, but this will be entirely at my own risk.When I use my*

personal devices in the Academy (PDAs/laptops/mobile phones/USB devices etc), I will follow the standards set out here, in the same way as if I was using Academy equipment. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses

- *I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering and security systems in place to prevent access to such materials*
- *I will not disable or cause any damage to Academy equipment, or the equipment belonging to others*
- *I will not store files unnecessarily, and shall ensure that I keep my file storage requirements to a minimum. I shall not store files on Academy systems that are unconnected with my work in the Academy*
- I will abide by the Data Protection Act, in particular only holding relevant personal data about others for as long as necessary and ensuring its security. I understand that any staff or student data to which I have access, will be kept private and confidential only on Academy devices and accounts; I shall not transport, hold, disclose or share personal information about myself or others except when necessary for the duties of my post within the Academy. I shall take special care when transferring data outside the Academy, and on these occasions ensure that it is always encrypted
- *I will immediately report any damage or faults involving equipment or software, however this may have happened*

Using the internet:

- *I will ensure that I have permission to use the original work of others in my own work*
- *Where work is protected by copyright, I will not download or distribute copies*

This agreement applies when:-

- *I use the Academy ICT systems and equipment (both in and out of the Academy)*
- *I use my own equipment in the Academy (when allowed) e.g. mobile phones, netbooks, cameras etc.*
- *I use my own equipment out of the Academy in a way that is related to me being a member of this Academy e.g. communicating with other members of the Academy, accessing Academy email, RealSmart tools, website etc.*

What can I do immediately?

- Change passwords regularly, especially you are watched by students. (Ctrl.Alt, Del > change password. At least 8 characters to include numbers or punctuation - no childs/partner names, dob, pets names etc)
- Make sure your network password and facility/eportal passwords are different in order that there are two layers of security protecting student data.
- Do not share passwords
- Do not let students use your laptop

- Lock office/classroom doors when absent
- Lock computer screens when leaving the desk (Ctrl, Alt, Del >Lock computer. Enter password to unlock)
- Report any evidence of misuse by students/staff to a member of the IT team
- Don't display personal/confidential data on projector screens
- Keep confidential paper in secure areas or locked away, shred when not required.
- Use remote access from home, do not transfer confidential data on staff or students via USB devices.

Parents and ICT Standards

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning.
We expect that parents will be partners with us in educating their children in the safe and responsible use of ICT. We look to parents to support their children:

- to become responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use
- to protect Academy ICT systems from accidental or deliberate misuse that could put the security of the systems and users at risk
- by being aware of the importance of e-safety and to be involved in the education and guidance of young people with regard to their on-line behaviour

The Academy will try to ensure that students will have good access to ICT to enhance their learning and will, in return, expect the student to agree to be responsible users.