E-SAFETY POLICY

Contents

Key List of Staff

Jason Beardmore
Iain Slade
Anna Winch
Chris Hayter

1. What is E-Safety?

Whilst the Internet and associated technologies are an excellent tool and resource to enrich learning there are still dangers related to their use, especially in relation to young students. Some examples of this are:

- Bullying via chat or email
- Obsessive internet use
- Exposure to inappropriate materials
- Inappropriate or illegal behavior
- Physical danger of sexual abuse or Child Sexual exploitation.

As an educational establishment it is our duty of care alongside that of parents/carers and other members of the community to protect our children from these dangers and this can be achieved by many different mechanisms working together.

The purpose of this e-safety policy is to outline what measures the academy takes to ensure that students can work in an e-safe environment and that any e-safety issue is detected and dealt with in a timely and appropriate fashion.

2. Audience

This document is intended for public consumption as well as that of academy members, parents/carers and local community and is a clear outward statement on the academy e-safety practices.

3. General policy statement

The academy will endeavor to ensure the e-safety of all academy members. It will use education, technology, accountability, responsibility and legislation as the key ways to achieve this.

4. Whole academy responsibilities for e-safety

Within the academy all members of staff and students are responsible for e-safety, responsibilities for each group include:

Students

- Participating in and gaining an understanding of e-safety issues and the safe responses from e-safety training sessions.
- Compliance with a highly visible student’s Acceptable Use Policy (AUP) which students must agree to each time they use academy ICT equipment either in the academy or remotely which connects to the internet.

- Reporting any e-safety issue to the teacher, pastoral team or parent.

- Take responsibility for their own actions using the internet and communications technologies in an acceptable manner.

All Staff

- Have a clear understanding of e-safety issues and the required actions from e-safety training sessions.

- Reporting any e-safety issues to the pastoral team and any child protection concerns to the Child Protection Lead Officer as soon as the issue is detected.

- Compliance with a highly visible staff Acceptable Use Policy (AUP) which staff must agree to each time they use academy ICT equipment either in the academy or remotely which connects to the internet.

Teaching Staff

- Educating students on e-safety through specific e-safety training sessions and re-enforcing this training in the day to day use of ICT in the classroom.

- Network Manager

- Ensure that the best technological solutions are in place to ensure e-safety as well as possible whilst still enabling students to use the internet effectively in their learning.

- Ensure that all information captured using these systems is secure, accessible to the appropriate members of staff, and stored in a robust manner. In addition securing and preserving evidence of any e-safety breach.

- Checks and audits all systems to ensure that no inappropriate data is stored or is accessible.

- Works with Safeguarding Lead and pastoral team to create, review and advise on e-safety and acceptable use policies.

Head of ICT

- Leads the development of the e-safety education program for students and staff.

- Manages a parental awareness programme for e-safety.

- E-Safety Lead

- Deals with e-safety breaches from reporting through to resolution in conjunction with the ICT support team.

- Works with the ICT Manager and ICT Director to create, review and advise on e-safety and acceptable use policies.

- Works with outside agencies including the police where appropriate.

- Maintains a log of all e-safety issues.

- ICT Support Team

- Monitors the technology systems which track student internet use to detect e-safety breaches.

- Assists in the resolution of e-safety issues with the E-Safety Manager and other members of staff.

5. How the academy ensures e-safety in the classroom

Educating students in e-safety

A clear objective of the academy is to educate students in safe use of ICT and the internet. We feel this is one of the best ways to minimise the potential for any e-safety issues to occur.

- Students will receive specific e-safety lessons aimed at ensuring that:

- Students know the e-safety risks that exists and how to identify when they are at risk.

- Students know how to mitigate against e-safety risks by using e-safe practices whilst online.

- Students know when, how and to whom to report instances when their e-safety may have been compromised.

- Students know that they are in an environment that encourages them to report e-safety issues without risk of reprimand, humiliation or embarrassment.

In addition to this specific training all members of staff will have a duty to reinforce e-safety practices wherever possible and will offer students advice and support in the classroom where minor e-safety incidents have occurred.

E-Safety education information will have high visibility in all areas of the academy.

Acceptable Use Policies

All academy members - students, staff and parents must agree to an Acceptable Use Policy (AUP) before they can use academy ICT systems. With respect to e-safety the AUP details:

- The user's responsibilities
- Activities which are appropriate and inappropriate
- Best practice guidelines
- How the academy will monitor e-safety
- What information is collected

How e-safety is monitored

- The ICT support team will actively monitor the students ICT activity using a monitoring system which can flag potential e-safety issues.
- The ICT team will periodically review internet access logs to track any websites which could potentially present an e-safety issue.
- The E-Safety manager will periodically review the E-Safety log to track and trends and use the information to look at ways of improving the student's e-safety.
- Teaching staff will directly monitor the students ICT and internet use in the classroom.

How technology is used

The academy will employ many different technologies to help to ensure e-safety for all the academy members;

- The academy will use internet filtering to block inappropriate content and in addition block websites which are irrelevant to the student's program of study and are considered time wasting.
- The Academy will use a system which tracks all student activity on the academy's computers. This system will automatically flags potential e-safety issues which will be monitored and then can be investigated.
- The academy will restrict which activities the students can perform using ICT and the internet through systems security policy and access control.
- Teaching staff will use control mechanisms to attempt to limit the applications and web sites which the students can visit whilst using ICT within a lesson.

6. How the Academy will respond to issues of misuse

The following are provided for the purpose of example only. Whenever a student or staff member infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the Principal.

Students:

Category A infringements

- Use of non-educational sites during lessons
- Unauthorised use of email
- Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends
- Use of unauthorised instant messaging / social networking sites

[Possible Sanctions: Dealt with by class teacher, /removal of phone until end of day / contact with parent/ removal of Internet access rights for a period]

Category B infringements

- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned
- Continued unauthorised use of mobile phone (or other new technologies) after being warned
- Accidentally accessing offensive material and not notifying a member of staff of it

[Possible Sanctions: referred to HOD / / Head of Year / removal of phone until end of week / contact with parent/ removal of Internet access rights for an extended period/ exclusion]

Category C infringements

- Deliberately corrupting or destroying someone's data, violating privacy of others
- Sending an email that is regarded as harassment or of a bullying nature (one-off)
- Deliberately trying to access offensive or pornographic material
- Any purchasing or ordering of items over the Internet
- Transmission of commercial or advertising material

[Possible Sanctions: referred to HOD / referred to HOY, E-safety // contact with parents / removal of equipment/ removal of Internet and/or Learning Platformaccess rights for an extended period/ exclusion/ referral to police]

Category D infringements

- Continued sending of emails or MSN messages regarded as harassment or of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the school name into disrepute

[Possible Sanctions – Referred to E-safety Manager/ Principal /exclusion / removal of equipment / referral to police / LA e-safety officer]

Staff:

Category A Infringements (Misconduct)

- Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
- Misuse of first level data security, e.g. wrongful use of passwords
- Breaching copyright or license e.g. installing unlicensed software on network

[Possible sanction - referred to line manager / E Safety Lead Principal / Warning given.]

Category B infringements (Gross Misconduct)

- Serious misuse of, or deliberate damage to, any school computer hardware or software;
- Any deliberate attempt to breach data protection or computer security rules;
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
- Bringing the Academy into disrepute.

[Possible Sanction – referred to Principal and follow Academy disciplinary procedures / Police/ GTC/ Governors]

Child Pornography:

In the case of child pornography being found, the member of staff will be immediately suspended and the Academy disciplinary procedures implemented.

Other safeguarding actions:

- Remove the PC to a secure place to ensure that there is no further access to the PC or laptop.
- Instigate an audit of all ICT equipment to ensure there is no risk of pupils accessing inappropriate materials in the school.
- Identify the precise details of the material.
- Where appropriate, involve external agencies as part of these investigations.

How will staff and students be informed of these procedures?

- Procedures are included within the school's e-safety / Acceptable Use Policy. All staff are required to sign the school's e-safety Policy acceptance form;
- Pupils will be instructed about responsible and acceptable use and given strategies to develop 'safe behaviors'. Pupils are required to sign an age appropriate e-safety / acceptable use form;
- The school's e-safety policy will be made available to parents who are required to sign an acceptance form when their child starts at the school.
- Staff are issued with the 'What to do if?' guide on e-safety issues.

7. Working with parents and the community

Clearly many academy students will also have access to ICT and the internet at home, often without some of the safeguards that are presents within the academy environment. Therefore parents must often be extra vigilant about their child's e-safety at home.

One of the goals of the academy is to support parent's role in providing an e-safe environment for their children to work in outside the academy.

The academy will do this in several ways;

- Run training sessions and workshops on e-safety.

- Publish e-safety information and direct parents to external e-safety advisories via the academy online parents portal and academy website.

8. Acceptable Use Policies

The academy has the following acceptable use policies in place which must be agreed to before the relevant individuals will be able to access ICT systems and the internet.

- Staff ICT and the Internet Acceptable Use Policy
- Students ICT and the Internet Acceptable Use Policy

A copy of these policies is available on request and can also be found in the Appendix. The academy will regularly review and update these policies.

Appendix

ICT Usage Policy

Including;

PT 1 - Information Security

- Information Security Policy

PT 2 - E-Safety, Internet Filtering & Monitoring

- E-Safety Policy
- Web Filtering Policy

PT 3 - Acceptable Usage

- Password Security Policy
- Student Acceptable Use Policy Agreement - to be signed and returned
- Staff (and volunteer) Acceptable Use Policy Agreement - to be signed and returned

Information Security Policy

1. Introduction

Stanchester Academy's investment in the acquisition, storage and use of electronic and paper based information exists primarily to help provide the effective delivery of its services. This information is held about a variety of people and it is essential that the availability and confidentiality of accurate relevant information is maintained in a secure and legal environment.

Stanchester Academy is committed to achieving policy requirements through an Information Security process. To actively demonstrate this we follow guidance of the local authority who has issued a Commitment Statement which provides assurance to students, parents, governors and staff that sound and secure measures are in place to protect the confidentiality, integrity and availability of their information.

2. Objective

The information security objective is to ensure that the Academy's information base is protected so that it may continue to deliver its services and obligations to the community. It also seeks to ensure that any security incidents have a minimal effect on its business and academic operations.

3. Policy

The purpose of this policy is to protect Stanchester Academy's information assets from all threats, whether internal or external, deliberate or accidental.

The key aims of the policy are to ensure that:

- information is protected from unauthorised access
- confidentiality of personal or sensitive information is assured
- integrity of information is maintained
- information is disposed of in a timely, appropriate and secure manner
- legislative requirements and Academy policy and practices are observed
- business continuity plans are produced, maintained and tested
- information security training is available to all Academy staff
- appropriate monitoring and reporting processes are put in place to identify and act upon breaches of information security

4. Supporting framework

In order to achieve this, Stanchester Academy will develop and maintain information security standards. These will be based on, but will not necessarily correspond in depth with ISO/IEC 27001 "Information technology – Security techniques – Information security management systems – Requirements" and ISO/IEC 27002 "Information technology - Security techniques - Code of practice for information security management"

Procedures, working practices and protocols will be maintained, either as detailed in ISO/IEC 27001 or as required by educational needs, to support this policy. Examples of measures to achieve the above are physical security, virus control and the use of passwords and encryption for access control. The development of any new system will include information security analysis and requirements as part of the initial specification and proposal.

5. Responsibilities

Stanchester Academy's Principal is responsible for ensuring the policy is maintained and ensuring appropriate advice and guidance on its implementation is provided. The Principal will also have responsibility for ensuring that the Academy's Senior Leadership Team and Governors receives an annual report on both the implementation and maintenance of the policy and its associated standards.

The Academy Senior Leadership Team and Heads of Department are responsible for ensuring the correct flow down and implementation of this policy and it is the responsibility of individual staff members to comply with the procedural directives of the policy.

6. Implementation

This policy will be made available to all students, parents, guardians, staff (whether permanent or temporary) and governors.

7. Review

The Academy's Principal, ICT Manager and Senior Leadership Team and Governors will review this policy annually and any changes necessary as a result of this review will be implemented.

PT 2 -

E-SAFETY, INTERNET FILTERING & MONITORING

Including;

- E-Safety Policy
- Web Filtering Policy

E-Safety Policy

Whilst the internet and associated technologies are an excellent tool and resource to enrich learning there are still dangers related to their use. Some examples of this are:

- Bullying via chat or email
- Obsessive internet use
- Exposure to inappropriate materials
- Inappropriate or illegal behavior
- Danger of sexual abuse

Our duty of care is to ensure that our students are protected whilst on our premises and in our care wherever that is. We also have a duty to prepare our students for use of these media aspects outside of the school and that is when we have joint care with the parents.

The purpose of this e-safety policy is to outline what measures Stanchester Academy takes to ensure that students can work in an e-safe environment and that any e-safety issue is detected and dealt with in a timely and appropriate fashion.

General policy statement

Stanchester Academy will endeavor to ensure the e-safety of our Students. It will use Education, technology, accountability, responsibility and legislation as the key ways to achieve this.

Web Filtering Policy

1. Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context.

The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that Stanchester Academy has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this Academy.
Stanchester Academy operates its own Web Filtering management system (Smoothwall) in conjunction with systems provided by South West Grid for Learning (SWGfL)

2. Responsibilities

Responsibility for the management of the filtering policy will be held by the ICT Manager who will manage Academy web filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems. Any breaches of the policy, either deliberate or inadvertently, will result in a documented investigation by the ICT Manager or a member of SLT (including a discussion with the individual) into how the breach occurred, why it occurred and how it can be prevented in the future. Any breach found to be deliberate would result in involving the Principal and either the disciplinary policy being followed for staff or the behavior policy for students.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the Stanchester Academy/SWGfL filtering systems will be recorded within those systems.

All users have a responsibility to report immediately to the ICT Manager any infringements of the Academy’s filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.
Users must not attempt to use any software to try to bypass the filtering / security systems in place to prevent access to such materials.

3. Education / Training / Awareness

Students will be made aware of the importance of filtering systems through

- e-safety education programme, assemblies and lessons
- signing the Acceptable Usage Policy

They will also be warned of the consequences of attempting to subvert the filtering system including potential damage to the schools infrastructure, other users work and that their actions could result in a breach of the behavior policy ultimately resulting in exclusion.

Staff users will be made aware of the filtering systems through:

- signing and returning the Acceptable Usage Policy
- induction training
- Staff meetings, briefings, Inset.

Parents will be informed of the Academy's filtering policy through the Acceptable Use Policy agreement and through e-safety awareness sessions and the Academy website.

4. Changes to the Filtering System

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to their Line Manager/Teacher who is responsible for reporting / requesting the site be blocked to the ICT Manger via the Launchpad. This report will be documented and a decision will be made whether to make Academy level changes (as above). If it is felt that the site should be filtered (or unfiltered) at SWGfL level, the ICT Manager can make these amendments on the SWGFL Portal

5. Monitoring

Stanchester Academy will monitor all student web access through Smoothwall Guardian Web Security software and Impero Classroom Monitoring Software. This software is designed to provide a safe environment for students whilst at the same time providing access to valuable education resources available online. An individual's web activity is constantly monitored, assessed and can be reported on as required.

No filtering system can guarantee 100% protection against access to unsuitable sites. The Academy will therefore monitor the activities of users on the Academy network and on Academy equipment as indicated in the Academy E-Safety Policy and the Acceptable Use agreement. Monitoring will take place as follows:

6. Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available on request to:

- *Senior Leadership Team*
- *SWGfL / Local Authority on request*

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

PT 3 -

ACCEPTABLE USAGE

Including;

- Password Security Policy
- Student Acceptable Use Policy Agreement - to be signed and returned
- Staff (and volunteer) Acceptable Use Policy Agreement - to be signed and returned

Password Security Policy

1. Introduction

Stanchester Academy will be responsible for ensuring that the network infrastructure is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user shall be able to access another's files, without permission (or as allowed for monitoring purposes within the Academy's policies).
- access to personal data is securely controlled in line with the Academy's personal data policy
- logs are maintained of access by users and of their actions while users of the system

2. Responsibilities

The management of the password security policy will be the responsibility of the ICT Manager.

All users will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

The IDM Support Team will allocate passwords for new users, and replacement passwords for existing users. Select ICT Curriculum Staff will also have the ability to reset a Students Password but no access to staff passwords.

3. Training / Awareness

Members of staff will be made aware of the Academy's password policy:

- at induction
- through the Academy's e-safety policy and password security policy
- through the Acceptable Usage Policy agreement

Students will be made aware of the Academy's password policy:

- in ICT and e-safety lessons
- through the Acceptable Use Agreement

4. Policy Statements

All users will have clearly defined access rights to Academy ICT systems. Details of the access rights available to groups of users will be recorded by the ICT Manager and will be

reviewed, at least annually, by the Principal, Senior Leadership Team and involvement of the Safeguarding Governors if necessary.
The IDM Support Team who will keep an up to date record of users and their usernames will provide all users with a username and password.

The following rules apply to the use of passwords:

- passwords must be changed every 90 days – you will be prompted of this
- the last two passwords cannot be re-used
- the password should be a minimum of 8 characters long and must include an uppercase, lowercase and a number
- the account shall be "locked out" following three successive incorrect log-on attempts
- temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on
- passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)
- requests for password changes should be authenticated by the member of staff who actions the change to ensure that the new password can only be passed to the genuine user

The master/administrator passwords for the Academy ICT systems, utilised by the ICT staff, will be made available to the Principal upon request and retained by the Head of Finance and kept in a secure place. Mark One LTD (an external ICT Support Company that provides ICT contingency & support to the Academy) holds a copy of these usernames and passwords.

5. Audit / Monitoring / Reporting / Review

The ICT Manager will ensure that full records are kept of:

- User Ids
- Security incidents related to this policy

In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption, with the appropriate legal authority i.e. a warrant.

User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner.

These records will be reviewed by SLT annually and this policy will be reviewed annually in response to changes in guidance and evidence gained from the logs.

Student Acceptable Use Policy

New technologies have become integral to the lives of children and young people in today's society, both within the Academy and in their lives outside of the Academy. The Internet and other digital information and communication 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. Young people should have an entitlement to safe Internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that students will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that Academy ICT systems, data and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that students respect physical ICT Equipment, do not intentionally damage it and report any damage immediately

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

Acceptable Use Policy Agreement

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.

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 not share my username or password, 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 unnecessary personal information about myself or others when on-line, and use a pseudonym/nickname where possible.
- 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

I understand that everyone has equal rights to use technology as a resource and:

- 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, this includes on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube) – this list is not exhaustive.

- I will not (unless I have permission or it is a curriculum requirement) download or upload excessively large files (including Videos, Music, Executable File and Archive Files – this list is not exhaustive or any excessively large file or files totaling over 500Mb. Any changes of this restriction will be made clear on the Launchpad) that might take up Internet capacity and prevent other users from being able to carry out their work.

I will act as I expect others to act toward me:

- 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 of anyone without their permission.

I recognise that the Academy has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the Academy:

- I will not connect my mobile phone, external hard-drive, or USB flash to any school machines unless given express permission to do so by a member of staff.
- 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 attempt to use any programs or software to try and 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.
- I will not open any attachments to emails, unless I know and trust the person / organisation that sent the email, due to the risk of the attachment containing viruses or other harmful programs.
- I will not install or attempt to install software of any type on Academy ICT equipment, nor will I download or attempt to store such software on the Academy servers
- I will not use or attempt to use chat or social networking sites within Academy.

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.

When using the Internet at home I recognise that:

- I must not use the internet in any way to attack or abuse fellow students or staff at Stanchester Academy
- I must not engage in activities on the internet which could bring Stanchester Academy's reputation into disrepute.
- Under no circumstances should offensive comments be made about Stanchester Academy, its staff or pupils, and I will report any such activity to a member of staff.
- The School reserves the right to monitor the usage of social media sites where there is a cause for concern

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

- 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 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 software monitors my ICT usage including Internet Monitoring, File Deletion and Inappropriate Language. Any examples of these will be documented and acted upon
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the Academy network / Internet, detentions, exclusions, contact with parents and in the event of illegal activities involvement of the police.

Student Acceptable Use Agreement Form

This form relates to the student Acceptable Use Policy (AUP), to which it is attached.
Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to Academy ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the Academy ICT systems and equipment (both in and out of Academy)
- I use my own equipment in Academy (when allowed) e.g. mobile phones, PDAs, cameras etc.
- I use my own equipment out of 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.

Student Name ____________________ **Student Signature**________________________

Parental Consent to use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Students and members of staff may use digital cameras to record evidence of activities in lessons and out of Academy. These images may then be used in presentations in subsequent lessons. Images may also be used to celebrate success through their publication in newsletters, on the Academy website and occasionally in the public media.

The Academy will comply with the Data Protection Act and request parents / carers permission before taking images of members of the Academy. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

To enable learning activities and promotional activities to take place we will make the assumption that you have no objection to your child taking part or their images being used.
If you have any objection to this please notify the Principal in writing:

Academy Office
Stanchester Academy
Stoke-sub-Hamdon
Somerset
TA14 6UG

As the parent / carer of the above students, I give permission for my son / daughter to have access to the Internet and to ICT systems at Stanchester Academy. I approve with the content of this agreement and am aware of my involvement should there be a breech of this agreement.

Parent / Carers Name ____

Parent / Carers Signature ____

Date of agreement ____

Staff, Governor (and Volunteer) Acceptable Use Policy Agreement

Academy Policy

New technologies have become integral to the lives of children and young people in today's society, both within Academy's and in their lives outside Academy. The internet and other digital information and communication 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. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

For you to fulfill your professional responsibilities you will need to know the appropriate use of the Academy's ICT provision. You have access to a wide range of ICT hardware and software for your professional use. The following summarises your responsibilities when using Academy ICT resources;

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that Academy ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.
- that users respect physical ICT Equipment, do not intentionally damage it and report any damage immediately

The Academy will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

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 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 will monitor my use of the ICT systems, email and other digital communications.
- I agree my Work E-mail Account can be checked without prior notification

- I understand that the rules set out in this agreement also apply to use of Academy ICT systems (e.g. laptops, email, VLE etc.) out of Academy.
- 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 immediately report any illegal, inappropriate or harmful material or incident; I become aware of, to the appropriate person.
- I will be professional in my communications and actions when using Academy ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express 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 and / or publish images of others I will do so with their permission and in accordance with the Academy's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the Academy website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in the Academy in accordance with the Academy's policies.
- I will only communicate with students / students and parents / carers using official Academy systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

Website & Internet Use

Only approved staff will update the Academy website.
The school website and any other kind of online information or communication portal is an extension of the workplace and should be treated in the same professional manner. No content should be submitted or made available that you would not share in a professional environment with Staff, Students or Parents.
All copyright laws will be followed.
Student photographs/images will be identifiable by name unless parent / carers opt out of Academy agreement (request through Academy Office).
The Academy and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the Academy:

- When I use a personal device PC/Laptop/Tablet or Mobile Phone to attach to the Academy Network I will follow the rules set out in this agreement, in the same way as if I was using Academy equipment. I will also follow any additional rules set by the Academy about such use. I will ensure that any such devices are protected by up to date anti-virus software where appropriate and are free from viruses.

- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programs.
- I will ensure that any data stored locally (laptops, USB flash drives) is regularly backed up.
- Any personal data will be held on an Encrypted USB Stick (available by request from the IDM Support Team) or data will be transferred to and from the Academy's Servers via VLE or VPN and not stored on any local machines when not being worked on.
- I will not try to upload, download or access any materials that are illegal, inappropriate or may cause harm or distress to others. I will not try to use any programs or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- 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, this includes on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube) – this list is not exhaustive.
- I will not (unless I have permission or it is a curriculum requirement) download or upload excessively large files (including Videos, Music, Executable File and Archive Files – this list is not exhaustive or any single file or collection of files over 500mb. Any changes of this restriction will be made clear on the Launchpad) that might take up Internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install software of any type on a machine, or store unlicensed software on a computer.
- I will not disable or cause any damage to Academy equipment, or the equipment belonging to others.
  I understand that data protection policy requires that any staff or student / student data, to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by Academy policy to disclose such information to an appropriate authority. Only current, relevant and accurate data will be stored and all current legislation will be implemented at all times.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the Internet in my professional capacity or for Academy sanctioned personal use:

- 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 (including music and videos).

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

- I understand that this Acceptable Use Policy applies not only to my work and use of Academy ICT equipment in Academy, but also applies to my use of Academy ICT systems and equipment out of Academy and my use of personal equipment in Academy or in situations related to my employment by the Academy.

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

Staff Acceptable Use Agreement Form

Staff confirmation of agreement Staff Acceptable Use Agreement Form

Staff confirmation of agreement

I have read and understand the above and agree to use the Academy ICT systems (both in and out of Academy) and my own devices (in Academy and when carrying out communications related to the Academy) within these guidelines.

Staff/Volunteer Name ____

Signed ____

Date ____