The Sutton Academy

E-Safety, Internet & Email Use Policy

Status	**Non-Statutory**
Responsible Governors' Committee	**HR & Finance**
Date last approved by GB	**02/10/2014**
Responsible Person	**Mr P Blakemore**
To Review Date	**January 2017**
Last Amended Date	**November 2016**

Title: E-safety, Internet & Email Policy

POLICY STATEMENT:

The E-safety Policy and ICT Code of Conduct policy is intended for students to provide guidance and clarity surrounding the access and use of computer equipment and other ICT-rich environments.

Scope of the policy and procedure:

The Policy and Procedure applies to all Academy Students

Associated Policies and Procedures and any other references:

Internet, E-mail and Protection of Data Policy

Access to the Policy:

This policy will be held on the academy website, accessible by all viewers.

Post - Holder to Contact

Paul Trainor –Assistant Principal

Recommendation:

That is for approval prior to sharing with the student body and inclusion on the Academy website.

Appendix 1 Authorization of Internet/email usage

Appendix 2 Notification for Removal of internet/email access

Appendix 3 Notification re Inadvertent access to Inappropriate Internet sites

Appendix 4 Notification borrowing or removal of Academy computer equipment from Academy premises

1. INTRODUCTION

- All reference to Academy In this document refers to The Sutton Academy, St Helens
- Reference to 'members of staff' includes volunteers, governors and other adults employed at the Academy.
- References to the Internet includes e-mail

1.1. The Internet is a very powerful tool for educational use. It does, however, present potential risks for staff, pupils and computer equipment used at the Academy. This policy has been developed to allow members of staff to make best use of the Internet whilst at the same time safeguarding members of staff and the Academy.

1.2. The purpose of this policy is to specify the rules in relation to staff use of the Internet, both within Academy and when using Academy equipment at home. The policy is provided to protect the Academy, its governing body, the user and the Council from risks associated with Internet usage. This Policy applies to all members of staff within The Sutton Academy.

2. STATEMENT OF POLICY INTERPRETATION IN RELATION TO THE INTERNET

2.1. Filtered access to the Internet in Academy is provided to members of staff in pursuance of their duties in Academy's. Access should only be attempted by members of staff who have been authorized to do so by the Head Teacher.

2.2. Members of staff using the Internet in Academy must do so within the general requirements of professional conduct. They should have particular regard to

Duty of Fidelity - this includes actions or omissions which could damage the business prospects or reputation of the Academy or in any way bring the Academy into disrepute.

Duty of Care - this is defined as carrying out *their particular occupation using the skills, ability and knowledge for which you are employed to the best interest of the Academy and using Academy equipment and resources with proper regard.*

Appropriate use of Academy Property or Facilities - staff must not remove or use Academy property for their personal requirements or for the benefit of others where the work of the Academy is not involved, unless permission has been granted from The Head Teacher or Assistant Head Teacher(ICT). Use of Academy buildings or facilities outside normal duties and hours of work must be fully authorized and open to scrutiny.'

2.3. E-mail communications, either internally or over the Internet, are not guaranteed to be private nor to arrive at their particular destination either within a particular time or at all.

2.4. Advice given on e-mail has the same legal bearing as any other written advice.

3. RULES GOVERNING INTERNET USE IN ACADEMY

3.1. The Principal will critically consider the granting of Internet access to ensure that usage will add value to the member of staff's role in the Academy. The Principal will also ensure that all members of staff are aware of the need for this authorization before attempting to use the Internet and that any unapproved connection may constitute a breach of the Code of Conduct.

3.2. The Principal will maintain a list of staff authorized to have access to the Internet, An authorization form must be completed for each member of staff, (Appendix 1). A copy should be kept on file at the Academy for each member of staff granted access. The Principal will immediately request the removal of Internet access for staff who leave and for any member of staff suspended from work.

The following rules must be adhered to when using the Internet:-

3.3. Internet access is provided to Academy through Virgin Media "BIG RED". The Academy provides an Internet firewall and filtering mechanisms. Members of staff should not attempt to circumvent or disable any of these features,

3.4. Members of staff should use their Individual I.D. when accessing the Internet and should not allow other staff or pupils to use their I.D. It is particularly important when logging on in front of pupils that staff ensure pupils cannot obtain the member of staff's password.

3.5. When logged onto their Internet account members of staff should not leave a workstation unattended unless it is locked.

3.6. All connections to the Internet, from within Academy, must be made through the Academy network unless specifically authorized by The Principal.

3.7. Members of staff should not use, or try to use, a Academy Internet account for intentionally accessing, displaying, storing or transmitting material that is obscene, sexually explicit, pornographic, racist, defamatory, hateful, that incites or depicts violence, or describes techniques for criminal or terrorist acts or otherwise represents values which are contrary to Academy policy. 1

3.8. Where access to such sites occurs accidentally this should be immediately reported to the Principal or the Senior Vice Principal or in the case of the Principal to the Chair of Governors. 2

3.9. Members of staff must be aware of and abide by the Data Protection Act as its provisions cover data transmitted and stored on e-mail.

1 Except where this is strictly and necessarily required by the job, for example where sexually explicit information is accessed to be used in the education/teaching of pupils

2 Principal or the Senior Vice Principal should note all such reported incidents on the appropriate form, (Appendix 3) to include the date, time, user and site(s) accessed. The Principal or the Senior Vice Principal on receiving such information will contact the Network Administrator and add the site to the list of banned sites, investigate and inform the relevant authorities as deemed appropriate.

3.10. Only those members of staff who are duly authorized by the Principal may publish content on electronic forums, upload software or upload data belonging to the Academy (e.g. web pages, application data).

3.11 The downloading or purchase of software must be subject to prior authorization, and in accordance with the Academy's financial regulations. All software should be properly licensed and registered.

3.12. The downloading of entertainment software, games, music or screen savers (other than for legitimate teaching purposes) is not allowed. Where legitimate downloading takes place it must not breach the rights of copyright owners.

3.13. Any orders placed via the Internet must first be authorized through the normal Academy financial procedures and in accordance with Financial Regulations and must be sanctioned by the Academy's business manager.

3.14. The playing of games against an opponent via the Internet is forbidden unless permission has been granted from The Principal.

3.15. The use of chat rooms, (other than those with a specific educational purpose) is forbidden.

3.16. Users should not use, or try to use, the Internet to break through security controls (i.e. hacking).

3.17. Users should not do anything which is illegal under English law or the law of any other relevant country.

3.18. Users should not use, or try to use an Academy Internet account for political lobbying.

3.19. Users should not use, or try to use, the Internet intentionally to access or transmit computer viruses or similar software.

3.20. Any software or files downloaded via the Internet become the property of the Academy.

3.21. E-mail users have a duty of care to protect the Academy, in accordance with professional conduct from any legal action for the likes of defamation, harassment, libel etc. resulting from staff use of the system.

3.22. Care should be taken when in receipt of unsolicited e-mail as it could be a vehicle for introducing viruses.

3.23. Care must be taken over the content of e-mails. It is important that the inclusion of personal information and of personal references to pupils should be avoided wherever possible. Under Data Protection Legislation, in the event of a Subject Access Request, personal data stored on e-mail is classed as relevant data and must be disclosed to the data subject.

3.24. In exceptional cases, where personal data is transmitted, appropriate security measures must be used (e.g. Encryption). Enterprise plc can advise Academys of the most appropriate method. All e-mails will carry the following disclaimer.

"This email and any attachments to it may be confidential and are intended solely for the use of the individual to whom it is addressed. Any views or opinions expressed are solely those of the author and do not necessarily represent those of The Sutton Academy. If you are not the intended recipient of this email, please notify the sender and delete it from your system. This email has been checked for viruses, but no liability is accepted by the academy for any damage caused by viruses which may have come from external sources."

4. PRIVATE USE OF THE INTERNET AND E-MAIL IN ACADEMY

The Head teacher will allow the private use of internet and e-mail in the Academy provided the following guidelines are adhered to:

4.1. All usage is governed by this Policy as outlined in Paragraph 3 *Rules Governing Internet Use.*

4.2. Access must be in the individual's own time and not in Academy time. This is defined as times when the employee is not actively involved in the fulfillment of their contractual obligations. There may be times in the normal working day where staff are freed from their contractual obligations such as lunchtimes, breaks or some specified free times as reasonably defined by the employer.

4.3. Personal use must be confined to viewing or browsing. There must be no storage of information, images, software unless this is to be used in conjunction with Academy work.

4.4. There must be no interaction (e.g. shopping, entering competitions, use of credit cards, financial services etc.) other than for Academy use in line with the financial policy of the Academy.

4.5. If permission is granted to send private e-mails using academy accounts then they should be dearly labelled as being private and not being sent as an official communication from and on behalf of the Council/Academy. The Council/Academy will not be held responsible for any fraudulent actions.

5. INTERNET ACCESS AT HOME USING ACADEMY EQUIPMENT

5.1. Some members of staff have access to Academy computer equipment (mainly laptop computers) which they are able to use at home. It is recognized that when using such computers within their own home staff will have greater freedom in relation to activities such as on-line shopping. When members of staff are using such equipment for personal use at home the following rules apply:

5.2. Members of staff should not use, or try to use, the Internet for intentionally accessing, displaying, storing or transmitting material that is obscene, sexually explicit, pornographic, racist, defamatory, hateful, that incites or depicts violence, or describes techniques for criminal or terrorist acts or otherwise represents values which are contrary to Academy policy. 3

5.3. Where access to such sites occurs accidentally this should be reported to the Principal or the Senior Vice Principal as soon as possible. 4 In the Case of the Head teacher it should be reported to the Chair of Governors.

5.4. Members of staff must be aware of, and abide by, the Data Protection Act as its provisions cover data transmitted and stored on e-mail.

5.5. Only those members of staff who are duly authorized by the governing body may publish Academy content on electronic forums or upload software or data belonging to the Academy (e.g. web pages, application data).

5.6. Any downloaded software should be properly licensed and registered. The downloading of music or data must not breach the rights of copyright owners.

5.7. Users should not use, or try to use, the Internet to break through security controls (i.e. hacking),

5.8. Users should not do anything which is illegal under English law or the law of any other relevant country.

5.9. Users should not use, or try to use, the Internet intentionally to access or transmit computer viruses or similar software.

5.10. The member of staff to whom the computer has been loaned is fully responsible for any use to which the machine is being put including access of the Internet. When members of staff are using such equipment for Academy business then the principles outlined in Paragraph 3 *Rules governing Internet Use* apply.

5.11. The Academy will not be held-responsible for any fraudulent actions

3 Except where this is strictly and necessarily required by the job, for example where sexually explicit information is accessed, in order to be used in the education/teaching of pupils. The person accessing such material should inform their line-manager about the exact nature and purpose of their work prior to undertaking such research.

4 This should normally be by the end of the next working day. The Head Teacher or ICT Co-coordinator should note all such reported incidents on the appropriate form, (Appendix 3) to include the date, time, user and site(s) accessed. The Principal or the Senior Vice Principal) on receiving such information will contact the Network Administrator and add the site to the list of banned sites, investigate and inform the LEA as deemed appropriate.

6. MONITORING OF INTERNET USAGE

6.1 Members of staff should be aware that all Internet access on any Academy device, both on and offsite is logged by our filtering hardware and that logs indicating the number and types of web sites that have been accessed by members of staff are subject to review by The Principal or the Senior Vice Principal.

6.2 Members of staff should be aware that all Internet activity, using academy e-mail accounts, are constantly monitored, through for inappropriate language and content.

6.3 Any inappropriate access/attempts to access, or e-mail activity will be investigated and may lead to disciplinary action being taken against members of staff. Disciplinary action may take the form of Gross Misconduct/Misconduct depending on the severity of the breach of the policy. Any inappropriate access of a criminal nature will be reported to the Police, or any other relevant agencies that the Governors deem appropriate.

6.4 There should be no expectation of privacy in Internet or e-mail usage by individuals.

6.5 The Academy reserves the right to inspect any and all files stored in private areas of the network or on disc in order to assure compliance with this policy.

6.6 In line with council strategy all logs of Internet usage are kept

indefinitely.

7 . The Sutton Academy Policy on Use of Social Media

7.1 A growing number of organisations in the public sector are using social media tools as an innovative way of engaging people in consultation and participative activities. Social media tools can be particularly useful in engaging with those who are not readily engaged using traditional participative tools.

7.2 Academies and Schools are now expected to lead the way in engaging with residents in local decision making and in improving and strengthening communities and neighbourhoods. Social Media will be vital in discharging these duties. It will allow us to engage with stakeholders in ways that they are familiar with. Through the use of social media we will have access to more innovative ways by which to communicate with the community using methods that are accessible, appropriate and cost effective.

7.3 The Academy recognises that it needs to embrace social media or it risks failing to engage with an increasingly large segment of the community.

7.4 The Academy will use Social Media tools to engage with the public where it is considered that such tools will provide an effective means of community engagement. However, safeguarding the reputation of the Academy will remain the key consideration in determining how and when Social Media is used.

The Purpose of the Social Media Policy

7.5 Social media presents the Academy with new opportunities to understand, engage and communicate with our residents. The potential of social media as a business tool is almost limitless, however if misused, it has the potential to cause considerable damage to the Academy, and to those we seek to engage with.

7.6 The most obvious examples of popular social media tools are now household names like Facebook, Twitter and YouTube. These facilities, and ones like them, have very rapidly changed the way in which individuals communicate with one another, increasingly overshadowing even e-mail accounts and text messages.

7.7 The purpose of this policy is to ensure that where the Academy uses social media, it does so in a controlled manner that enables us to engage safely and

effectively with residents and other parties.

7.8 The policy seeks to ensure that the reputation of the Academy is not adversely affected through our use of social media, and that the Academy is not exposed to legal and governance risks that can be very significant.

Overview

What is Social Media?

7.9 There is no current legislative definition of a social network, although the Office of Communications (Ofcom), who regulate the environment describe social networks as
'…sites which allow users to set up on-line profiles or personal homepages and develop an on-line social network. The profile page functions as the users personal web page and includes profile information ranging from date of birth… …to what they like doing in their spare time'

7.10 Social media is the term we commonly give to websites and online tools that allow users to interact with each other. This interaction can be by sharing information, opinions, knowledge, music, images, links to other websites and a host of other activities.

7.11 As the name implies, social media involves the building of communities or networks, encouraging participation, engagement and cohesion.

7.12 It should also be recognised that smaller, 'industry specific' networks that Academy officers may be participating in are also social networks.

Risks from Inappropriate use of Social Media

7.13 The power of social media also carries considerable organisational risk. The ease in which individuals can place information and opinion in a very public domain means that its use has to be appropriately controlled. As an organisation, we place strict control over who can place information on our own website, or who can contribute directly to the press. It is important that these controls equally apply to our use of social media.

7.14 It is important that the Academy is able to use these tools effectively but equally important that our duties to our service users, our legal responsibilities and our reputation are protected.

7.15 Our use of social media applications has implications for our duty to safeguard children, young people and vulnerable adults. There is a duty of care to protect the Academy from any legal action arising from defamation, harassment, libel, or discrimination, and we must operate within the guidelines of the Academies Equality and Diversity Policy.

7.16 This Policy seeks to provide this balance by providing a framework of good practice that supports innovation.

Scope

7.17 This policy covers the use of social media tools by Academy employees and bythird parties and contractors acting on behalf of the Academy. These groups are referred hence forth collectively as 'Academy representatives'.

7.18 Where individuals from partner organisations are involved and are acting on

behalf of The Sutton Academy, they will also be expected to comply with this policy.

7.19 Contractors, third parties and partners are also expected to ensure that private use of social media by their employees will not be conducted in a way which could damage the reputation of the Academy or could be considered harassment, intimidation or bullying of Academy students or employees.

Terms of Use of Social Media

General

7.20 Academy representatives must adhere to the following Terms of Use. The Terms of Use below apply to all uses of social media tools by all Academy representatives.

7.21 This includes, but is not limited to, public facing applications such as open discussion forums and internally facing uses such as project blogs regardless of whether they are hosted on corporate networks or not.

7.22 Where applications allow the posting of messages online, users must be mindful that the right to freedom of expression attaches only to lawful conduct. The Sutton Academy expects that users of social media tools will always exercise the right of freedom of expression with due consideration for the rights of others and strictly in accordance with these Terms of Use.

7.23 In particular, Social Media must not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claims for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the Academy into disrepute.

7.24 When representing the Academy representatives should identify themselves as such where appropriate on social media tools. This would include providing additional and appropriate information in user profiles.

7.25 Academy representatives should ensure that any contributions they make are professional and uphold the reputation of the Academy and are in accordance with the conditions of this policy.

7.25 When using Social Media at home for personal use, staff must follow the following guidance:

- On Facebook, privacy settings must be set so that students cannot find your profile. Guidance on how to set these are appendices…
- On twitter, "Tweets" must be protected and privacy settings at a level where permission has to be sought for them to be viewed. Guidance on how to set these are appendices…
- On any form of Social Media, staff should not be communicating with current students or former students under the age of 21. This includes being "friends" on Facebook or being "followed/following" on twitter. It alos includes all other Social Media such as Instagram.
- Conduct on Social Media such be professional and staff should be aware that their behaviour on Social Media indirectly reflects on the Academy. Comments made, statements written or even posts liked can reflect poorly and staff should be aware of this.
- Social media must not be used in a manner that breaches the Academies misconduct and bullying and harassment policies.

Compliance with Conditions of Use of Social Media Providers

7.26 This section applies where social media tools are provided by third parties.

7.27 The largest social media tools such as Facebook are international commercial enterprises. While there is often no financial cost to the Academy in using them, they are each an independent legal entity and are entitled to impose strict conditions of use.

7.28 Representatives of The Sutton Academy must abide by the conditions of use imposed by any provider of social media they wish to use.

7.29 The Sutton Academy representatives must never attempt to circumvent the conditions imposed by a social media provider in order to secure a presence in a particular area.

7.30 The risk of this is that the social media provider may shut down our presence without notice and any customer contact details would be lost. They may also seek legal redress, which may have a financial and reputational impact.

7.31 In particular, where a social media provider imposes restrictions on corporate participation that are more stringent than those regarding individuals, Academy representatives must never attempt to circumvent this by assuming an individual identity.

7.32 If a Academy representative cannot participate in a particular social media while complying with its conditions of use, and within the rules imposed by this policy, then that particular social media provider will be deemed inappropriate.

7.33 The ICT Regulation and Compliance team within Internal Audit will advise the Academy on the appropriateness of the conditions of use of individual social network providers.

Data Protection

7.34 The Academies obligations under Data Protection legislation are significant, and are aimed at protecting individuals from any damage through inappropriate capturing, maintaining or disclosure of information. Penalties for breaching data protection legislation are significant.

7.35 The capacity to reach a worldwide audience with instant communication through social media means that there is a significant data protection risk associated with its inappropriate use.

7.36 In managing a social media tool Academy representatives may publish or refer to material from a wide range of sources, including that drawn from within the Local Authority and Sponsors. Equally, Academy representatives may receive comments, enquiries or complaints from members of the public through social media.

7.37 Both published and received material may contain personal data. St Helens Academy is committed to full compliance with the law and to the welfare of individuals and therefore any such personal data should be treated with care

7.38 Anyone processing personal data must comply with the principles of good practice contained that relate to material published and correspondence received.

7.39 Material published through social media is potentially accessible to anyone in the world. It is essential to restrict the publication of personal data, which includes facts and opinions about individuals. Only that data for which explicit consent for publication has been obtained, or that is clearly already, and properly, in the public domain can reasonably be published.

7.40 Correspondence using social media creates electronic records and, as such, individuals are entitled to access these records if they hold information about themselves.

7.41 In the event of a **"Subject Access Request"** being made by an individual, Academy Representatives will be required to provide copies of relevant emails. All requests must be satisfied within 40 calendar days of receipt of the request.

7.42 Further details about the principles of good practice may be found at: http://www.dataprotection.gov.uk/dpr/dpdoc.nsf

7.43 Academy Representatives must consult the Academies Internal Audit section wherever they feel that social media activity may have implications with regard to Data Protection legislation.

Safeguarding Vulnerable People

7.44 Representatives of the Academy must bear in mind that the information they share through social media, including through private spaces, remains subject to legal requirements governing publication and disclosure, including the Safeguarding of Vulnerable Groups Act (2006).

e-Safety and Communicating with Vulnerable people on-line

7.45 Any use of a social media tool that is specifically targeted at engaging with young people, or other vulnerable people including vulnerable adults needs to be mindful of good practice guidance, including advice from St Helens Safeguarding Children Board, and St Helens Safeguarding Adults Board.

7.46 Any proposal for the use of social media to engage specifically with young people needs to be highlighted as part of the approval process.

7.47 Any background checks that are required under the Safeguarding Vulnerable Groups Act 2006 must be satisfied and relevant information recorded by the appropriate manager. This is particularly relevant to any services aimed at children, young people and vulnerable adults.

7.48 A condition of that approval will be that administrators and moderators will receive training on e-safety and in appropriate communication with young and vulnerable people on line.

7.49 On-line communication also brings risks that include contact with people who may wish to cause offence or harm, cyber-bullying through images and messages, and access to obscene or offensive contact.

7.50 The use of social media to engage with young people should not target potential users who are under the minimum age of the service being used, nor should users be asked to divulge any personal details including home and e-mail addresses, telephone numbers or anything that may identify the location of the person.

7.51 Although the majority of current e-safety advice focuses on young people, e-safety issues can potentially affect all people who use online services, particularly vulnerable adults who may be at a higher risk of being persuaded to share sensitive personal information

7.52 e-Safety awareness is also crucial for professional staff who may be at risk of misrepresentation and malicious accusations through social networking.

Obligations under Equalities Legislation and the reporting of hate crimes

7.53 Social Media must not be used in an abusive or hateful manner, or in such a way that breaches the Academies obligations under equality and diversity legislation (Race Relations (Amendment) Act 2000)

7.54 This includes the content of public and private social media tools. It includes messages, images or other information that may be posted by Academy representatives. Importantly, it also covers the hosting of posts by other parties on social media sites relating to Academy activity.

7.55 Where the Academy receives electronic material through social media that is in contravention with legislation in respect of Hate Crime, or incitement to such, we will report this to the Police without hesitation or exception.

Responsibilities regarding potential criminal activities

7.56 The Academy is bound by the legislative requirements of the Anti-Terrorism, Crime And Security Act 2001 to report to the police any activity, or suspicion of activity relating to terrorism or incitement to such that may arise through our use of social networking tools.

7.57 The Academy may also share with the police any information regarding actual or potential criminal activity of any kind received through social media.

Obscene Publications

7.58 The publication of obscene material is prohibited by the Obscene Publications Act 1959; the Protection of Children Act 1978 and the Criminal Justice Act 1988)

7.59 This legislation will apply to material and images that may be posted by third parties on social networking sites hosted by the Academy.

7.60 Arrangements must be in place to prevent the Academy from hosting any such material or images posted by third parties on hosted social networking sites.

Use of User-ID's and e-Mail Addresses and Academy Branding

7.61 It is important to ensure that members of the public and other users of online services know when a social media tool is being used for official Academy purposes. To assist with this, all Academy Representatives must adhere to the requirements contained within this section:

7.62 Any social media website or link that is being officially used by the Academy should be explicitly referred to on a section of the Academy (http://thesuttonacademy.org.uk) website homepage or social media page, so that users of online services can determine if content on a site or link is being legitimately provided by the Academy.

7.63 Academy representatives must only use @thesuttonacademy.org.uk email for user accounts that will be used for official Academy purposes, unless this is specifically prohibited by the application being employed;

7.64 In certain circumstances (e.g. www.facebook.com), alternative email accounts can be used, however these must use an email naming convention agreed by the IT Support and in line with existing naming conventions.

7.65 These email accounts may be used for username logins only and must never be displayed on any website or otherwise made public.

7.66 The use of the Academy logo and other branding elements should be used where appropriate to indicate the Academy support.

7.67 The logo, or other devices must never be used on social media tools that are unrelated to, or are not representative of, the Academy official position or which do not conform to the conditions within this Policy.

Feedback, Complaints and Requests for Information

7.68 Where Academy representatives are managing social media tools, appropriate feedback and complaints information must be published in a prominent place, which is easily accessible to other users.

7.69 Service requests, complaints and comments made by users via social media tools should be referred to the Academies Contact Centre.

7.70 Communication regarding these enquiries must not be dealt with through social media. Only direct communication methods, such as e-mail and telephone can be used, in accordance with out professional standards.

Freedom Of Information Requests

7.71 The Freedom of Information Act 2000 may apply to requests received through

Social Media. This may require Academy Representatives to disclose information when presented with such a request.

7.72 Any Freedom of Information request made by users via social media should be referred to the Academies Customer Contact Centre.

7.73 Communication regarding these enquiries must not be dealt with through social media. Only direct communication methods, such as e-mail and telephone can be used, in accordance with our professional standards.

Press and Media Requests for Comments

7.74 Requests for statements from the Academy or press enquiries through social media should be referred directly to the Principal, and managed accordingly.

Publication of Music, Images and Video Clips through social network sites

7.75 Any music, image or video footage published by Academy representatives through a social media outlet must be from an appropriate and approved source.

7.76 Academy representatives must ensure that images or audio and visual material published through a social media outlet do not infringe copyright requirements.

7,77 Academy representatives must be mindful of the need for permission and consent where images of individuals, particularly children, are shared through social media.

The Role of the Moderator

7.78 A Social Media Moderator is one of the most important and difficult roles to undertake. The main role for the allocated moderator will be to see that any comments posted comply with the guidance provided to participants and allow the Academy to conduct social media activity in accordance with this policy.

7.79 The Moderator of any social media tool will be the individual who ensures that no material is published, either by ourselves *or by third parties*, that will contravene our responsibilities under this policy, in particular:

i. disclosure of personal information in contravention of the Data Protection Act;
ii. material of an offensive nature;
iii. images of a pornographic or otherwise offensive nature;
iv. material that is of a racial, homophobic or otherwise discriminatory nature, and that may constitute incitement;
v. material of a defamatory nature;
vi. material that breaches our safeguarding responsibilities; and
vii. any other inappropriate material of the type considered in section 4 above.

7.80 This is in addition to encouraging and nurturing an on-line community and trying to ensure that the aims of the social media presence are delivered by the on-line debate or forum.

7.81 Any department that wishes to use a social media tool must carefully consider who is selected to carry out this role, and the effect that it may have on their normal duties.

7.82 Moderation needs to be appropriately resourced, in particular on 'open forums' where third parties may post material directly for public viewing at any time of the day or night.

Types of Moderation

7.83 There are three main methods of moderating social media applications. The type of moderation that is selected should depend on the outcomes required from the proposed use of social media, and an assessment of risk.

7.84 The type of moderation should never be determined by the terms of a particular social media provider. If that provider does not allow the type of moderation that is deemed appropriate by the Academy, then an alternative method of communication should be employed.

7.85 The Academy can exercise the most control over material posted to its social media sites by undertaking moderation before posts are made available to a wider audience. This involves all posts being intercepted by the Moderator, who then exercises a right of veto prior to wider publication.

7.86 This offers the greatest protection against inappropriate or offensive material appearing on our social media presence, however it is not appropriate to all applications. It is a closed process, which may be considered disengaging and which does not lend itself to real-time discussion and debate. There is also an issue with capacity, and this is only suitable in a relatively small online community.

7.87 A further type of moderation is to seek registration from potential users before

allowing participation. In this environment, would-be users need to satisfy some form of registration and identity requirements before they are allowed to participate. Once registered, they can post freely within the terms defined by the owner of the forum, however should they breach these terms, the Moderator can withdraw access rights, and in extreme cases report any criminal activity to the Police.

7.88 This type of moderation is used by many organisations as a way of balancing the need to encourage debate with the reputational risks associated with allowing un-moderated access. Many of the most successful on-line organisations such as the BBC, national newspapers and forums such as 'Mumsnet' and St.Helens RLFC's 'RedVee' forum take this approach. It is also employed by smaller specialist networks of the type commonly used by professional groups.

7.89 This approach works well where the popularity of the site, or the benefits associated with participation are considered to be worth the effort of registering by users. This may not always be the case for Academy activity, particularly around promotion, marketing and consultation.

7.90 The third type of moderation occurs where access to a site is open to a wide community, without the need to register, and where users may post material directly for public view. This is the approach that is inherent when using Facebook and Twitter in particular.

7.91 In such instances, the risk of carrying inappropriate or offensive material is greatest, and moderators need to be vigilant in frequently checking posted material and removing offending posts as soon as possible. This is particularly important when using Twitter, as although 'tweets' can be deleted, this may occur after they have been forwarded ('re-tweeted') to many other users from our feed.

7.92 Where Twitter, Facebook and other similar tools are employed, the Academy needs to ensure that arrangements for moderation are robust and are appropriately well resourced.

Guidance for Moderators

7.93 Guidance for Moderators will be specific to the type of social media that is employed, however it will be based on the principles of this policy.

Enforcement

7.94 The Regulation and Compliance team within Internal Audit, in consultation with the relevant Senior Manager and the Academies Head Finance, reserves the right to require the closure of any applications or the removal of any content published by Academy representatives which they deem may adversely affect the reputation of the Academy or place it at risk of legal action.

7.95 Any breach of this Policy could result in the use of the social media tool or offending content being taken away (in accordance with the published complaints procedure), and the publishing rights of the responsible Academy representative being suspended or permanently removed.

7.96 Any communications or content that causes damage to the Academy, any of its employees or any third party's reputation may amount to misconduct or gross misconduct to which the Academies Disciplinary procedures apply.

ADVICE AND POLICY INTERPRETATION

If you are uncertain about any aspect of the above Policy and its application please contact the Academy's Assistant Head Teacher (ICT)
If you wish to report any violations of this policy you should inform The Head Teacher or Assistant Head Teacher (ICT). You will be dealt with in complete confidence.

Any violations of the above policy will be thoroughly investigated and may result in disciplinary proceedings and if necessary criminal proceedings.

E-safety Policy and ICT Code of Conduct

E-safety

The Academy has a duty of care to ensure that Information and Communications Technology (ICT) is used appropriately and does not compromise the safety of staff and students or the reputation of The Academy.

The Internet and other digital and information technologies are powerful tools which open up new learning opportunities for everyone. These technologies can stimulate discussion, promote creativity and increase awareness of context to
promote effective learning. It is the Academy's intention to provide Students with an entitlement to safe internet access at all times.

The Academy is committed to ensuring that all our students are able to use the Internet and related communications technologies appropriately and safely.

E-Safety Training Awareness

The Academy provides E-Safety awareness training for parents, students and staff. Undertaken by our CEOPs Ambassador (Mr Stockley) training is offered during our Year 6 Induction Evening as well as to staff as part of the Masterclass CPD programme (compulsory attendance for all NQTs and ITTs).

ICT Code of Conduct

For users of computers at The Sutton Academy:

The Academy computer systems are the property of the Sutton Academy. Users (authorised or unauthorised) have no explicit or implicit expectation of privacy. By logging onto The Academy systems you are agreeing to abide by the Academy's rules governing the use of its ICT equipment.

Any or this entire network and any files housed within it or shared across it may be intercepted, monitored, recorded, copied, audited, inspected and disclosed to The Director of Network Services and law enforcement personnel, as well as other authorised officials. By using the Academy's ICT system the user consents to such interception, monitoring, recording, copying, auditing, inspection and disclosure at the discretion of authorised Academy staff.

What you may use the Academy's computer equipment for?
Computers are provided solely for academic purposes. All users **must** adhere to the following rules:

- Don't waste materials, or waste time on the computers to the detriment of others.
- Don't send offensive or unsolicited junk or nuisance mail. Also remember mail might accidentally reach somebody for whom it was not intended.
- Your use must be lawful, honest and decent, and must have regard to the rights and sensitivities of other people.

This means that any use that is obscene or with the intent of annoying or offending somebody else is forbidden.

• Don't use the Academy's computers for commercial gain.
• Don't bring into the Academy computer games, viruses, public domain software, shareware software or devices containing any offensive material.
• The law requires you don't hold any information in electronic form about living persons unless you are registered to do so.

Respect Computer Suites:
• Please treat computer equipment with respect - it is there for your benefit. Do not tamper, attempt to repair or remove any of the equipment.
• Please be considerate of other computer users - avoid excessive noise or other nuisance.
• No eating or drinking in ANY classroom or near the iMac Suites located in the Technology Street.
• Don't run your own software on the Academy's PCs or load software on to the computers' hard discs unless you have explicit permission to do so.
• Don't delete, disable or tamper with any software provided by the Academy.
• Don't tamper with the hardware or any network or power connections.
• Avoid unnecessary printing. Proof read and spell check a file prior to printing and only print single copies of your work.
**Please note that the Academy reserves the right to seek to recover financial costs of repairs from anyone that wilfully damages the computer equipment or associated peripheral devices (including network ports).

Using the Network:
• Never attempt to gain access to an account (username or file store) on another computer unless you have been given permission to do so. If you do you may be in direct breach of the law and the rules supported by the Academy.
• Don't connect your own equipment to the network except in approved locations provided for that purpose (this includes, but it not exclusive to, mobile phones and music players).
• All students are entitled to register to use the PC network.

Username and Passwords:
When you join the Academy you receive a unique username and password upon your receipt, please keep this safe;
• It is your responsibility to keep your username and password secure. Never allow anyone else access to it.
• Keep your password secret. You will be asked to change your password upon first login. Don't use anything that someone might guess about you. If you have to write it down, disguise it. Remember to change your password regularly. If you think someone might have watched you typing it in, change it immediately.
• Don't leave a logged in session unattended, event for a moment.
• Make sure you log out when you finish using the computer.
• Never use anyone else's account, with or without their permission.

Looking after your data:

You, not the Academy, are ultimately responsible for the security of your data. Wherever possible, keep an independent copy of your data. Power, disc and system failures usually take effect without warning.
Think about the consequences before you use the computers!

The following good practice is recommended:

• Save your files at frequent intervals.
• Keep your own multiple backup copies of anything that is important.
• Pen drives and similar technologies are also compatible with the majority of the systems within the Academy.
• Network storage areas are given to every account.
• Observe Copyright restrictions

• Don't copy any software without permission. You should assume software is copyright unless you know otherwise.
• Don't copy any data without permission. This includes copying text or graphics (whether using a scanner of typing it in) and also includes the downloading or uploading of copyrighted images, sound and music and multimedia works. The usual exceptions to copyright arrangements, which allow you to photocopy parts of an article or books, do not apply to the use of computers.

Rules and discipline:

If you break any of the above guidelines, the Academy reserve the right to remove your privilege to use the computer system, network, Internet, VLE and associated computer hardware. Staff should be aware that any breach of the rules set out in this policy may result in a disciplinary investigation, in accordance with the Academy's Code of Conduct Policy.

Printing:

All students are asked to help the Academy reduce costs and waste by making sure that you carefully proof-read your work prior to printing. You should only print essential work and print only the number of copies that you are asked for by your teacher.

Appendix 1

AUTHORISATION OF INTERNET/E-MAIL USAGE

Name: _____

Post Held: _____

Authorisation is granted for Internet/e-mail use in accordance with the Internet/e-mail policy adopted by the Academy.

I have read and understood the policy and agree to access the internet/e-mail system in accordance with the policy.

Signed: _____

Printed Name: _____

Date: _____

Authorised by Head Teacher: _____

Date: _____

Appendix 2

NOTIFICATION

REMOVAL OF INTERNET/E-MAIL ACCESS

Name: _____

Post Held: _____

Date Access is to cease: _____

Authorised by Head Teacher: _____

Date: _____

Appendix 3

NOTIFICATION

INADVERTENT ACCESS TO INAPPROPRIATE INTERNET SITES

Name: _____

Post Held: _____

Site accessed: _____

Date of Access: _____

Time of Access: _____

Reported by: _____

Authorised by Head Teacher/Assistant Head Teacher (ICT):

_____

Date: _____

For Internal Use

Investigated by: _____

Date: _____

Action Taken:

_____
_____
_____
_____

Appendix 4

NOTIFICATION

Borrowing or Removal of Academy Computer Equipment from Academy Premises

Name: _____

Post Held: _____

Equipment Description: _____

Serial Number: _____

Date of Removal: _____

Expected return date: _____

Authorised by Head Teacher/Assistant Head Teacher (ICT):

_____

Date: _____