E SAFETY POLICY

LAST REVIEW NEXT	**October 2020**	**REVIEW PERIOD**	**Annually**
NEXT REVIEW DATE	**October 2021**	**OWNER**	
TYPE OF POLICY		**APPROVAL LEVEL**	

Contents

" The Internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners.

To use these technologies effectively requires an awareness of the benefits and risks, the development of new sills, and an understanding of their appropriate and effective use both in and outside of the classroom." DfES, eStrategy 2005.

Academy Policy

This Policy document is drawn to protect all parties – our/your children, our staff and our Academy. The aims of which are to provide clear advice and guidance on how to minimise the risks and how to deal with any infringements

What is E-Safety?

1. E- Safety is often defined as 'the safe and responsible use of technology' this includes:
    a. The use of the internet and other means of communication
    b. Using electronic devices (e.g. iPad/tablets/laptops/mobile phones/ cameras etc.)
    c. Social media
    d. Gaming
    e. Email
2. In the context of an inspection, e- safety is described as the academies ability to:
    a. Protect and educate staff and pupils in their use of technology
    b. To have the appropriate safeguarding mechanisms to prevent, monitor, intervene and support any incident where appropriate

Risks within e-safety can be categorised as follows:

1. Content:
    a. Exposure to inappropriate content
    b. Content promoting harmful behaviour
    c. Hate content
    d. Content validation: how to check authenticity and accuracy of online content
2. Contact:
    a. Grooming (sexual exploitation, radicalisation, extremism)
    b. Online bullying in all forms
3. Conduct:
    a. Aggressive behaviours (bullying)
    b. Privacy issues, including disclosure of personal information
    c. Digital footprint and online reputation
    d. Health and wellbeing (amount of time spent online, gambling, body image)

Scope of Policy

This policy applies to all members of Sutton House Academy Community, including employees, pupils, volunteers, parent/carers, visitors) who have access to and are users of the Academy ICT systems both in and outside the Academy.

The Education and Inspections ACT 2006 empowers Headteacher, to such extent as is reasonable, to

regulate the behaviour of pupils when they are off the Academy site and empowers members of staff to impose disciplinary sanctions for inappropriate behaviour. This is pertinent to incidents of cyberbullying or other e-safety incidents covered by this policy, which may take place out of the Academy, but are linked to the Academy. Please note this policy should be read in conjunction with the Safeguarding & Child Protection Policy, Anti-Bullying Policy and Staff Code of Conduct.

The Academy will deal with incidents using guidance within this and will inform parents/carers of any e-safety incidents.

Roles and responsibilities:

Role	Key Responsibilities
Advisory Board member responsible for e-safety	• Annual meeting with E-safety Co-ordinator/committee • Termly monitoring of E-safety incident logs • Regular monitoring of filtering/change control logs • Reporting to Advisory Board
Headteacher/SLT	• Has a duty of care for safeguarding all members of the PLT community by ensuring robust implementation of up to date safeguarding policies across the Academy. • The day-to-day responsibility for e-safety will be delegated to the Designated Safeguarding Lead and the e- safety Co- coordinator. • The principle should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff • The Headteacher is responsible for ensuring that the e-safety Coordinator and other relevant staff are e-safety trained to carry out their roles and train other colleagues. • Head Teacher supported by senior leader's senior leaders will ensure there is a system in place to allow for monitoring and support for all those who carry out the internal monitoring role. • SLT to ensure that e-safety is taught and embedded in the curriculum
Designated Safeguarding Lead	• Will deal with any of the safeguarding issues that might arise from: • Sharing of personal data • Access to illegal/ inappropriate materials • Inappropriate on-line contact with adults/ strangers • Potential or actual incidents of grooming • Cyber-bullying • Any breach of the e safety and associated safeguarding policies. • Provides regular quality assurance reports to the Headteacher and SLT.
E-safety Coordinator	• Leads the e-safety committee • Take the day to day responsibility for e-safety issues with the safeguarding lead • Has a leading role in establishing and reviewing the Academy's e-safety policies/documents • Ensures that all staff are aware of the procedures to be followed in the event of an e-safety incident taking place. • Receives reports of e-safety incidents from the safeguarding lead and create a log of incidents to inform future training. • Reports regularly to DSL / SLT • Ensures any concerns raised by staff about E safety practices are

	investigated and where appropriate sanctions are applied.
Network Manager/ Technical staff	• Ensure that the Academy's technical infrastructure is secure and is not open to misuse or malicious attack • Meets all the e-safety technical requirements and any Local Authority/other relevant body E-safety policy and guidance that might apply. • Ensures that users may only access the networks and devices through a properly enforced password protection policy and passwords are regularly changed.
Teaching and Support Staff	• Have attended training in E safety. • Have access to and have read the e safety policy. • Have read, understood and signed the Staff Code of Conduct for ICT. App 1. • Receive regular refresher training and updates in E Safety Policy and procedures. • Report any concerns about E safety to the DSL / E safety Co-coordinator for investigation. • Ensure that: o all digital communications with pupils/parents/carers should be on a professional level and only carried out using the official Academy's systems o E- safety issues are embedded in all aspects of the curriculum and other activities o Pupils understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so o Pupils have a good understanding of research skills and the o need to avoid plagiarism and uphold copyright regulations o They continuously monitor the safe use of digital technologies, cameras, iPads etc. in lessons and other activities. o In lessons where internet is used, sites must be checked and suitable for the pupils use and inform technical staff if any unsuitable material appears. o Staff do not share their passwords with pupils to passwords to access the internet.
AGENCY SUPPLY STAFF Teaching and Support	• Must read the staff handbook on the first day as an induction prior to undertaking any duties • Must have read and signed the staff code of conduct for ICT • Must be familiar with and comply with the Academy mobile phone policy • Must know who the DSL and DCPO are and how to contact them.
E- Safety committee	• Consultative group which has a wide representation from the Academy • Monitoring and review the e-safety policy • Monitor and review the impact of e-safety in the curriculum • Report to the DSL.
Pupils	• Are responsible for using the Academy technology systems in accordance with the **student Acceptable Use Policy** • Are responsible for avoiding plagiarism and uphold copyright regulations.

	• Are responsible reporting abuse, misuse or access to inappropriate materials.
Parents/Carers	• To read, understand and promote the Academy's the Student • Acceptable Use Agreement with their child where appropriate • To consult the Academy if they have any concerns about their child's use of technology • Support the Academy in promoting online safety and endorse the **parent Acceptable Use Agreement which includes the pupils use of photographic and video images**
Community Users	• Any external individual/organisation will sign an Acceptable Use Agreement prior to using technology or the internet within the Academy • To model safe, responsible and positive behaviours in their own use.

Education and Curriculum

1. Student's online safety curriculum

   Sutton House Academy constantly develops its progressive online safety education programme as part of the curriculum / PSHE. This programme covers a range of skills and behaviours appropriate for the age, needs and experience of pupils. The Academy:

   - Constantly re enforces Key e-safety as part of a planned programme of awareness raising activities such as assemblies, tutor and teaching programme
   - Ensures that pupils are taught to be critically aware of the potential safeguarding risks posed by materials/content they access online
   - Ensures staff model safe and responsible behaviour in their own use of technology e.g. use of internet, passwords, logging off, use of content

2. Education – Parents/Carers

   Parents and carers play an essential role in the education of their children and in the monitoring/regulation of their online behaviours, yet many have a limited understanding of the risks and issues e-safety risks and issues. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

   Sutton House Academy provide information and awareness to parents and carers through:

   - Appointment of a Parent Safeguarding Champion
   - Newsletter
   - Letters and publications from agencies such as NSPCC and CEOP
   - Academy website provides information and signposting.
   - Safeguarding workshops for Parents / Carers
   - PLT Open Support Forum

3. Education Staff/volunteers/ Governors training

   It is essential that all staff receive training and understand their responsibilities, as outlined in

this policy. Training will be offered as follows:

- An e- safety audit will be carried out annually
- A planned programme of formal e-safety training will be made available to staff.
- All new staff should receive e-safety training as part of their induction programme and fully understand the Acceptable Use Agreements.

Illegal or inappropriate activities and related sanctions:

1. Sutton House Academy deem the following activities are inappropriate and users should not engage in these activities when using Academy equipment or systems whether on site or off site. NB: those activities in bold are illegal.

2. Users should not visit internet sites, post or download, data transfer, communicate or pass on material, remarks, proposals or comments that certain or relate to:
   - Child sexual abuse images (The Protection of Children Act 1978)
   - Grooming, incitement, arrangement or facilitation of sexual acts against children (illegal- Sexual Offences Act 2003)
   - Possession of extreme pornographic images (Criminal Justice and immigration Act 2008)
   - Criminally racist material in UK- to stir up religious hatred, hatred on the grounds of sexual orientation, gender bias of disability bias. (Public Order Act 1986)
   - Pornography
   - Promotion of any kind of discrimination
   - Promotion of radicalisation or extremism
   - Threatening behaviour, including promotion of physical violence or mental harm
   - Any other information, which may be offensive to colleagues, breaches the integrity of the ethos of the Academy, or brings the Academy into disrepute.

3. In addition to the above, the following activities considered unacceptable on ICT equipment or infrastructure provided by the Academy:
   - Using the Academy systems to undertake transactions pertaining to a personal / business use.
   - Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed the Academy
   - Uploading, downloading or transmitting commercial software or any copyrighted materials
   - Belonging to third parties, without the necessary licensing permissions
   - Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)
   - Creating or propagating computer viruses or other harmful files
   - On-line gambling and non-educational gaming
   - On-line shopping / commerce
   - Use of social networking sites (other than in the Academy's learning platform or sites otherwise permitted by the Academy.

4. If members of staff suspect that misuse might have taken place – whether or not it is

evidently illegal (see above) - it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. All such concerns must be communicated to Headteacher and/or Designated Safeguarding Lead.

5. It is more likely that the Academy will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that Academy staff are aware that incidents have been dealt with. Incidents of misuse will be dealt with through the Academy Staff Code of Conduct and disciplinary procedures.

	Refer to:					**Inform:**	**Action:**		
Pupil Sanctions	Class Teacher	E-Safety Co-ordinator	Refer to Headteacher	Refer to Police	Refer to E-Safety Co-ordinator for action re filtering/security etc.	Parents/Carers	Removal of the network internet access rights	Warning/Sanction	Further sanction e.g. detention/exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).	✓	✓	✓	✓	✓	✓	✓	✓	✓
Unauthorised use of non-educational sites during lessons	✓	✓			✓			✓	
Unauthorised use of mobile phone / digital camera / other handheld device	✓	✓				✓	✓	✓	
Unauthorised use of social networking / instant messaging / personal email	✓	✓			✓	✓	✓	✓	
Unauthorised downloading or uploading of files	✓	✓			✓	✓	✓	✓	
Allowing others to access Academy network by sharing username and passwords	✓	✓			✓			✓	
Attempting to access the Academy network, using another pupil's account	✓	✓			✓			✓	
Attempting to access or accessing the Academy network, using the account of a member of staff	✓	✓	✓		✓	✓		✓	
Corrupting or destroying the data of other users	✓	✓			✓	✓		✓	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓		✓	✓	✓	✓	
Continued infringements of the above, following previous warnings or sanctions	✓	✓	✓			✓	✓		✓
Actions which could bring the Academy into disrepute or breach the integrity of the ethos of the Academy	✓	✓	✓			✓		✓	✓

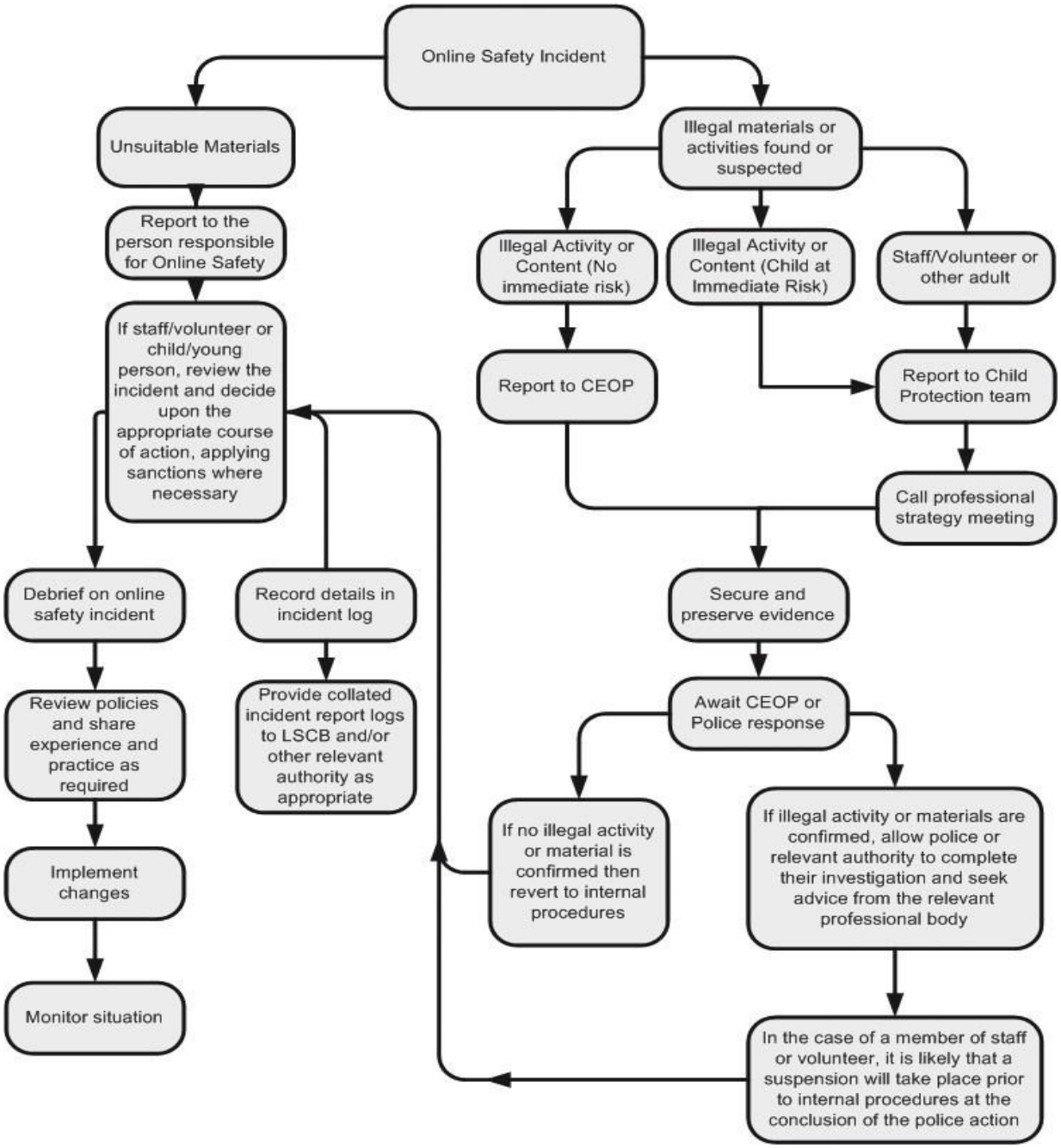
Using proxy sites or other means to subvert the Academy's filtering system	✓	✓			✓		✓	✓	
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓			✓	✓			
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓	✓		✓	✓		✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✓	✓	✓		✓	✓	✓		✓

	Refer to:					**Action:**		
Staff sanctions	Line Manager	Headteacher	Safeguarding	Police	Technical support staff for action re filtering etc.	Warning	Suspension	Disciplinary Action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓	✓	✓	✓	✓	✓	✓
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	✓	✓				✓		
Unauthorised downloading or uploading of files	✓	✓			✓	✓		
Allowing others to access Academy network by sharing username and passwords or attempting to access or accessing the Academy network, using another person's account	✓	✓			✓	✓		
Careless use of personal data e.g. holding or transferring data in an insecure manner	✓	✓			✓	✓		
Deliberate actions to breach data protection or network security rules	✓	✓			✓	✓	✓	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✓			✓		✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓			✓	✓		
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils / pupils	✓	✓	✓		✓	✓		
Actions which could compromise the staff member's professional standing	✓	✓						

Actions which could bring the Academy into disrepute or breach the integrity of the ethos of the Academy	✓	✓						
Using proxy sites or other means to subvert the Academy's filtering system	✓				✓			
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓	✓		✓	✓		
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓	✓	✓	✓	✓	✓
Breaching copyright or licensing regulations	✓	✓				✓		
Continued infringements of the above, following previous warnings or sanctions	✓	✓			✓			✓

Reporting of e-safety breaches

Sutton House Academy expect that all members of the Academy community are responsible users of ICT, with a regard for this policy at all times. However, there may be times when infringements of the policy occur through careless or irresponsible misuse or occasionally, through deliberate misuse. Academy responses to any apparent or actual incidents of misuse are set out below:



Use of hand held technology (personal phones, tablets and other hand held devices)
Members of staff are permitted to bring their personal mobile devices into Academy. They are required to adhere to the following policy requirements:

- Personal hand held devices must be kept in a safe place in the staff room or, where there is not access to a designated staff room; a designated safe place on site. Staff must not carry a mobile phone or any other personal internet device or camera outside of the staff room/designated area during the academy day. The only exception to this rule is the Senior Leadership Team, who will ensure mobile phones are kept out of site at all times.
- Staff are able to use these devices during break periods within the staff room area.
- Academy mobile phones are available for professional use, or example when engaging in off-site activities. Staff should follow the e safety policy and not make visible, or use their personal device at any time during an off-site activity, except in an emergency.
- Pupils must hand over hand held devices to staff for safekeeping during security checks upon entry to the building at the start of each day. Devices will be kept is a designated safe space and returned to the pupil upon their departure from the building at the end of the day. Devices including iPads, tablets and cameras are provided by the Academy for staff and pupils to use in all learning related activities. These devices should not be used for personal use.

Use of communication technologies

- Email
    - Access to Academy email is provided for all users in the Academy.
    - Academy email services may be regarded as safe and secure and are monitored.
    - Staff should use only the Academy email services to communicate with others when in Academy.
      NB: Members of SLT may use Academy supplied mobile devices to e mail when working from home, or working in the community.
    - Staff should only access personal email accounts on Academy systems for emergency or extraordinary purposes. Staff may access personal e mails on personal devices such as smart phones during official breaks in the staff room area only.
    - Users are advised that the Academy has the right to monitor e mail systems.
    - A structured education programme is delivered to pupils which helps them to be aware of the dangers of and good practices associated with the use of email
    - Users must immediately report to their class teacher / E-Safety Coordinator, in accordance with the Academy policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and they must not respond to any such email.

Social networking (including chat, instant messaging, blogging etc.)

	Staff				Pupils			
Use of social networking tools	Allowed	Allowed at certain time	Allowed for selected staff	Not allowed	Allowed	Allowed at certain time	Allowed with staff member	Not allowed
Use of non-educational chat rooms etc.				✓				✓
Use of non-educational instant messaging				✓				✓
Use of non-educational social network sites				✓				✓
Use of non-educational blogs				✓				✓

Use of digital and video images

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Members of staff are allowed to take digital still and video images to support educational aims, but must follow Academy policies concerning the sharing, distribution and publication of those images. Those images should only be captured using Academy equipment; the personal equipment of staff should never be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the Academy into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.

Use of web-based publication tools

- Academy Website
  Sutton House Academy uses the public facing website www.suttonhouse.org.uk for sharing information with the community beyond our Academy. This may include celebrating the work, sports activities and achievements of pupils. All users are required to consider good practice when publishing content.
    - Personal information will not be posted on the Academy website and only official email addresses will be used to identify members of staff (never pupils).
    - Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images:
        - pupils' full names will not be used anywhere on a website or blog, and never

in association with photographs
- where possible, photographs will not allow individuals to be recognised
- written permission from parents or carers will be obtained before photographs of pupils are published on the Academy website

Professional standards for staff communication

Sutton House Academy expect all teachers abide by the broad Professional Standards for Teachers laid down by the TDA effective from September 2012 in all areas of their work.

Teachers are expected to translate these standards appropriately for all matters relating to e-safety.

- Digital communication between staff and pupils or parents / carers (parent mail, email and chat) must be professional in tone and content.
- Communications must only take place on official monitored Academy systems.
- Personal email addresses, text messaging or public chat / social networking technology must not be used for these communications.

Staff are expected monitor and evaluate developing technologies, considering risks and benefits, for learning and teaching. These evaluations help inform policy and develop practice.

Password security

The Academy's e-safety curriculum will include frequent discussion of issues relating to password security and staying safe in and out of the Academy. Staff and pupil passwords are confidential. Staff and pupils alike, are responsible for ensuring they do not share passwords with anybody.

Internet Security Filtering Systems

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 the Academy has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this Academy.

   Sutton House Academy's broadband provider, TrustNet, effects robust filtering of all websites. In addition, the Academy Network Manager is able to filter websites and liaises regularly with TrustNet ensuring safeguarding mechanisms are secure.

2. Responsibilities

   The day-to-day responsibility for the management of the Academy's filtering policy is held by the Network Manager. Overarching responsibility rests with the Headteacher and Advisory Board.

   All users have a responsibility to report immediately to class teachers / E-Safety Coordinator / DSL 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 programmes or software that might allow them to bypass the filtering/ security systems in place to prevent access to such materials.

3. Education / training / awareness

The Academy e safety education programme ensures pupils are aware of the importance of filtering systems.

Staff users are made aware of the filtering systems through:

- signing the ICT Code of Conduct (as part of their induction process)
- Briefing in staff meetings, training days, safeguarding updates, memos etc.

Parents are able to access the Academy e-safety policy on the Academy website and hard copy on request. Induction meetings include reference to the policy, specifically the E-safety Code of Conduct Agreement.

4. Changes to the filtering system

Where a member of staff requires access to a website that is blocked for use at Academy, the process to unblock is as follows:

- The teacher makes the request to the Network Manager
- The Network Manager checks the website content to ensure that it is appropriate for use in the Academy.

In turn:

The Network Manager unblocks the site and logs the action in the change-control log, which is made available to the SLT and the Advisory Board.

The Network Manager will need to apply a rigorous policy for approving / rejecting filtering requests, ensuring that the requested site:

- Promotes equal and just representations of racial, gender, and religious issues.
- Does not contain inappropriate content like pornography, abuse, racial hatred or terrorism.
- Does not link to other sites which may be harmful / unsuitable for pupils.

5. Monitoring

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.

Monitoring takes place as follows:

- The Network Manager reviews the monitoring console on a weekly basis and reports to the DLS on a monthly basis.
- "False positives" are identified and deleted
- Potential issues are referred to the DSL or Headteacher.

- Teachers are encouraged to identify in advance any word or phrase likely to be picked up regularly through innocent use (e.g. Essex is captured frequently when a class is researching local history, news) so that the word can be allowed for the period of the topic being taught.

6. Audit / reporting

Filter change-control logs and incident logs are made available to:

- SLT via the DSL termly
- The e-safety governor termly.
- The LSCB on request

This filtering policy will be reviewed, with respect to the suitability of the current provision, in response to evidence provided by annual audits and/or emerging issues.

Managing complaints regarding E-Safety.

Sutton House Academy will take reasonable precautions to ensure E-Safety. However, the international scale of the internet together with easy access to mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on an Academy computer or mobile device. Neither the Academy nor the Local Authority can accept liability for material accessed, or any consequences of internet access.

The Academy in conjunction with the Local Authority, monitors all activity and use. This includes all types of text from word document's written to web pages viewed, with infringements reported to the Executive Head teacher, after which staff or student(s) concerned are given information about infringements in use and possible sanctions.

Sanctions may include:

- Informing students, parents or carers
- Referral to Local Authority or police
- Removal of internet or computer access for a period (which ultimately prevent access to files held on the system)
- The e-safety co-ordinator will act a first point of contact for any complaint
- Any complaint about staff misuse is referred to the Headteacher

Complaints of cyber bullying are dealt with in accordance with our Anti-Bullying Policy.

Complaints related to child protection are dealt with in accordance with Academy/Local Authority child protection procedures.

APPENDIX 1
Staff Code of Conduct for ICT

To ensure that staff are fully aware of their professional responsibilities when using information systems they are expected to sign this code of conduct.

I have read and understood the 'Academy E Safety Policy - Nov 17'.

I understand that it is a criminal offence to use an Academy ICT system for a purpose not permitted by its owner - PLT

I appreciate that ICT includes a wide range of systems, including mobile phones and all hand held devices, digital cameras, email, social networking.

I understand that Academy information systems may not be used for private purposes.

I understand my use of Academy information systems, Internet and email may be monitored and recorded to ensure policy compliance.

I will respect system security and will not disclose any password or security information to anyone other than the Network Manager.

I will not install any non SLT approved software or hardware onto PLT devices.

I will ensure that PLT data is stored securely and is used appropriately, whether on site or off.

I will not engage in any form of electronic communication with or about pupils, past and present. This includes on social media, even if the post is not made by me.

I will not interact with social media sites during the academy day. This includes during breaks.

I will ensure that personal communication and social networking are secure and not accessible/open to students and/or their families.

I will ensure that I do not make reference to PLT Sutton House or Sutton House Academy on social networking sites.

I will not post inappropriate messages and/or images on social networking sites that may bring the Academy into dis repute and in breach of Academy Safeguarding Policies.

I will promote e-Safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing in accordance with the e-Safety Policy.

I have read, understood and accept the Staff Code of Conduct for ICT.

Name: _____ Role: _____

Signed: _____ Date _____

APPENDIX 2
Student E Safety Code of Conduct

E- Safety is 'the safe and responsible use of technology' this includes:

- Any form of communication via the internet, including posting images, video's and messages on social media sites, through gaming sites and by use of e mail.
- Use of electronic devices (e.g. I pads/tablets/laptops/mobile phones/ cameras

Whilst the Internet and associated technologies present great opportunities for learning and socialising, they also present serious risks.

E safety guidelines to help us stay safe:

- I will only go online when I have been given specific permission by staff do to so.
- I will only log on to websites that have been authorised by staff.
- I will not bring in USB sticks or other storage devices from outside academy unless I have been given permission
- I will not share my login details with anybody else and I will only use my login details to log on to the internet.
- If I access something inappropriate by accident, I will inform staff immediately. (Inappropriate includes sites of a violent and sexual nature).
- I understand that using academy devices such as laptops and tablets to access social networking sites e.g. Facebook is not allowed at any time.
- I will not post or send any information by e mail or text, that is rude, abusive or upsetting to anyone.
- If I receive any messages that make me feel bullied or upset, I will inform a member of staff or an adult and take steps to block the sender.
- I understand that my academy may check my computer files and may monitor the sites I visit
- I will always hand in my mobile phone to the office or give it to a teacher to lock in the cupboard when I come into the academy building.

I have read, understood and accept the Pupil E Safety Code of Conduct.

Name: _____ Signature: _____ Date: _____