Manchester Communication Academy

E-Safety

with you, for you, about you.

This document has been approved for operation within	
Date of last review	
Date of next review	
Review Period	Every two years
Date of Trustee Approval	
Status	
Person Responsible for Policy	
Owner	Manchester Communication Academy
Signature of Approval	

Introduction

The Byron Review "Safer Children in a Digital World" stressed the role of schools and academies:

"One of the strongest messages I have received during my Review was about the role that schools and other services for children and families have to play in equipping children and their parents to stay safe online. To empower children and raise the skills of parents, I make recommendations to Government in the following areas: delivering e-safeguarding through the curriculum, providing teachers and the wider children's workforce with the skills and knowledge they need, reaching children and families and taking steps to ensure that Ofsted holds the system to account on the quality of delivery in this area."

The development and expansion of the use of ICT, and particularly of the internet, has transformed learning in schools in recent years. Children and young people will need to develop high level ICT skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment. There is a large body of evidence that recognises the benefits that ICT can bring to teaching and learning. Schools have made a significant investment both financially and physically to ensure these technologies are available to all learners. The benefits are perceived to "outweigh the risks." However, schools must, through their e-safeguarding policy, ensure that they meet their statutory obligations to ensure children and young people are safe and are protected from potential harm, both within and outside school. The policy will also form part of the trust's protection from legal challenge, relating to the use of ICT.

Due to the ever changing nature of Information and Communication Technologies, it is best practice that the trust reviews the e-safeguarding policy annually and, if necessary, more frequently in response to any significant new developments in the use of the technologies, new threats to e-safeguarding or incidents that have taken place.

Background

Background New technologies have become integral to the lives of children and young people in today's society, both within the trust and in their everyday lives.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students learn from one another. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in the trust are bound including the PREVENT duty. A trust e-safeguarding policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the Principal and Governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students themselves.

The use of these exciting and innovative tools in the trust and at home has been shown to raise educational standards and promote student achievement. However, the use of these new technologies can put young people at risk.

Some of the dangers they may face include: •

- Access to illegal, harmful or inappropriate images or other content including materials relating to radicalization
- Unauthorised access to/loss of/sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video/internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world which is why this policy sits alongside other Trust safeguarding policies.

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

The Trust will demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safeguarding policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Schedule for Development, Monitoring and Review

This e-safeguarding policy has been developed by the e-safeguarding forum:

- Andrea Grant – Safeguarding Officer and Governor
- Alex Garry – Teacher of Computing
- Mark Farrimond – System Manager
- Kate Coey – Data Officer

This e-safeguarding policy was approved by the Governing Body on:	
The implementation of this e-safeguarding policy will be monitored by:	E-safeguarding forum
Monitoring will take place:	Once every half term
The e-safeguarding forum will receive a report on the implementation of the e-safeguarding policy, which will include anonymous details of e-safeguarding incidents, at regular intervals:	Once every half term
The e-safeguarding policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safeguarding or incidents that have taken place. The next anticipated review date will be:	July 2019
Should serious e-safeguarding incidents take place, the following persons should be informed:	Andrea Grant (GMAT Assistant Principal Safeguarding) Greater Manchester Police (Moston)

The e-safeguarding forum will monitor the impact of the policy using: •

- Logs of reported incidents on CPOMS
- Monitoring logs of internet activity including sites visited from Smoothwall
- Monitoring of inappropriate email activity using Google Tools
- Internal monitoring data for network activity using Net Support
- Surveys of students, parents/carers and staff

Scope of the Policy

This policy applies to all members of the trust community (including staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of trust ICT systems.

The Education and Inspections Act 2006 empowers Principals to regulate the behaviour of students when they are off the trust site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safeguarding incidents covered by this policy, which may take place out of trust, but is linked to membership of the trust.

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

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safeguarding of individuals and groups within the trust:

E-safeguarding Forum

The Principal/Head is responsible for ensuring the safety (including e-safeguarding) of members of the Trust community, though the day to day responsibility for e-safeguarding will be delegated to the e-safeguarding forum.

The forum is responsible for the implementation of the e-safeguarding policy and for reviewing the effectiveness of the policy. This will be carried out by the forum receiving regular information about e-safeguarding incidents and monitoring reports. The role of the e-safeguarding forum will include:

- Regular meetings
- Regular monitoring of e-safeguarding incident logs
- Regular monitoring of filtering/change control logs
- Reporting to Governors through the Safeguarding Officer

The forum is also responsible for ensuring all staff receive CPD to enable them to carry out their role.

The Principal/Head and other members of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safeguarding allegation being made against a member of staff.

The Safeguarding Officer and Assistant Principal/Head

- leads the e-safeguarding committee

- takes day to day responsibility for e-safeguarding issues and has a leading role in establishing and reviewing the trust e-safeguarding policies and documents.
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safeguarding incident taking place.
- provides induction, training and advice for staff
- liaises with trust ICT technical staff
- receives reports of e-safeguarding incidents and creates a log of incidents to inform future e-safeguarding developments
- Reports to Governors
- Reports to the relevant Principal/ SCITT AO:
    - Is responsible for dealing with the following incidents:
    - sharing of personal data
    - access to illegal/inappropriate materials –
    - any incident relating to the PREVENT duty –
    - inappropriate on-line contact with adults or strangers –
    - potential or actual incidents of grooming –
    - cyber-bullying

The System Manager is responsible for ensuring that:

- The trust's ICT infrastructure is secure and is not open to misuse or malicious attack
- The trust meets the e-safeguarding technical requirements outlined in the e-safeguarding policies •
- Users may only access the trust's networks through a properly enforced password protection policy, in which passwords are regularly changed
- The trust's filtering policy, is applied and updated on a regular basis and that its implementation is shared with the Data/Web Technician
- The Trust keeps up to date with e-safeguarding technical information in order to effectively carry out their e-safeguarding role and to inform and update others as relevant
- The use of the network is monitored in order that any misuse is reported to the forum
- Monitoring systems are implemented and updated

Teaching and support staff (including trainees) are responsible for ensuring that:

- They have an up to date awareness of e-safeguarding and of the current trust e-safeguarding policy, practices and processes
- They report any suspected misuse or problem to the e-safeguarding Co-ordinator for investigation.
- Digital communications with students via email, VLE or other trust services should be on a professional level
- Students understand and follow the trust e-safeguarding and acceptable use policy
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons and extended trust activities
- they are aware of e-safeguarding issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current trust policies with regard to these devices

Students

- are responsible for using the trust ICT systems in accordance with the student AUP (age related) which they will be expected to sign before being granted access •
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

- will be expected to know and understand trust policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand trust policies on the taking/use of images and on cyberbullying
- should understand the importance of adopting good e-safeguarding practice when using digital technologies outside of the trust and realise that the trust's e-safeguarding policy covers their actions out of trust, if related to their membership of the trust

Parents and carers

Parents play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The trust will therefore take every opportunity to help parents understand these issues through parent evenings, newsletters and website. Parents and carers will be responsible for endorsing (by signature) the student AUP.

Community Users

Community users who access trust ICT systems / website / VLE as part of the Extended Trust provision will be expected to sign a Community User AUP before being provided with access to trust systems.

Policy Statements

Curriculum – Students

The education of students in e-safeguarding is an essential part of the trust's e-safeguarding provision. Students need the help and support of the trust to recognise and avoid e-safeguarding risks and build resilience.

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

- A core e-safeguarding programme will be provided as part of the new Computing curriculum
- This will be developed in the Project 60 curriculum and will cover both the use of ICT and new technologies in and outside the Trust
- Key e-safeguarding messages will be reinforced as part of a planned programme of House time activities
- Students will be taught in all lessons to be critically aware of the materials/content they access on-line and will be guided to validate the accuracy of information
- Students will be helped to understand the need for the student AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both in and outside the Trust
- Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

Training – Parents and carers

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

The trust will provide information and awareness to parents and carers through:

- Newsletters
- Parent section of the trust website

- Parent evenings
- E-safety workshops and drop ins
- Trust e-safety App

The trust will also offer family learning courses in ICT and e-safeguarding so that parents and children can together gain a better understanding of these issues. Messages to the public around e-safeguarding should also be targeted towards grandparents and other relatives as well as parents. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

Training – All staff/ Trainees

All staff/ trainee will receive e-safeguarding induction and training to enable them to understand their responsibilities, as outlined in this policy.

Training will be offered as follows:

- A planned programme of formal e-safeguarding training will be made available to staff •
- All new staff should receive e-safeguarding training as part of their induction programme, ensuring that they fully understand the trust e-safeguarding policy and Acceptable Use Policies

Training – Governors

Governors will take part in e-safeguarding awareness sessions.

Student ICT Agreement

The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Student ICT Agreement will ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use. •
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

I will....

- Switch my mobile telephone off when in lessons.
- Protect and look after all ICT equipment.
- Only use ICT equipment and resources for trust work.
- Always ask permission when using my own DVDs, CDs, USB drives or ICT equipment.
- Protect my work by keeping my password to myself and never use someone else's logon name or password.
- Remember that the trust monitors my use of the ICT systems and digital communications and stores some data on Google cloud with enhanced security.
- Not open attachments or click on links in emails unless I know and trust the person who sent it.
- Not install or attempt to install programmes of any type on a computer or try to alter computer settings.

- Ensure that I have permission to use the original work of others in my own work or where work is protected by copyright, I will not try to download copies including music and videos.
- Only access suitable material from the Internet for my trust work and not use the Internet to search, download, send, print, display any materials which are unlawful, obscene or abusive.
- Respect the work from people outside of the trust when working online.
- always get permission before giving my home address, telephone number, trust name, or picture to people I may meet on the Internet.
- Always ask a parent or teacher to go with you if you need to meet someone who you only know from the Internet.

Please read this document carefully. Once it has been signed and returned to the trust access to the Internet be allowed. If you break any of the rules you will be asked to attend an interview with the pastoral team, your parents may be informed and access to ICT equipment and the Internet may be denied. In serious cases you may be suspended, the police may be involved or other legal action taken. I have read and understand the above and agree to use the trust ICT facilities within these guidelines.

Student name: _____
Signature: _____

I have read the above and discussed it with my child.

Parent name: _____
Signature: _____

Staff ICT Use – Quick Guide

The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. 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.

This guidance will ensure:

- Staff, trainees and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use. •
- School ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk. •
- Staff/ trainees are protected from potential risk in their use of ICT in their everyday work.

Equipment

- Mobile telephones should not be used and business emails should not be accessed whilst teaching.
- Trust ICT facilities should only be used for educational purposes.
- Seek the support of the IT Support Team if software needs to be installed. •
- Protect the IT equipment from spillages by eating or drinking well away from ICT equipment.

Security and Privacy

- The use of ICT systems and digital communications is monitored by the trust in response to the PREVENT duty.
- Passwords should be kept private - never logon as someone else or logon for a student.

- Computer storage areas are the property of the trust. The IT Support Team may review user areas and files to ensure the responsible use of equipment and services.
- Images of others should only be taken on trust equipment, with their permission, in accordance with the policy on the use of digital/video images.
- When personal data is transferred outside the secure school network, it must be encrypted as outlined in the Personal Data Policy.
- The Data Protection Policy requires that staff access to any staff/ trainee or student data will be kept private and confidential.

Internet

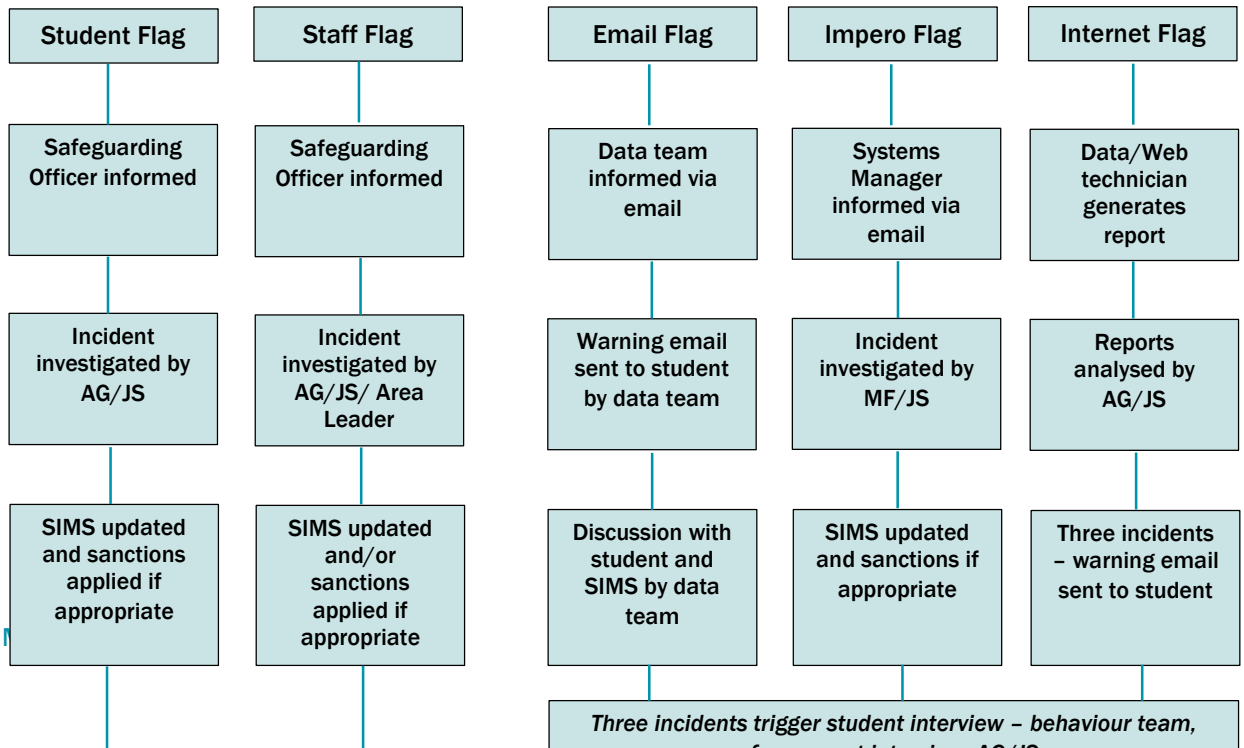
- The use of Facebook and other social networking sites to discuss trust business is not allowed. Privacy settings should be set so only friends can see profiles.
- Only access the Internet for trust work.
- Only access suitable material; using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.
- Report to the Safeguarding Officer in the unlikely event of accessing inappropriate content.
- Respect the work and ownership rights of people outside the Trust, as well as other students or staff. This includes abiding by copyright laws.

Email

- Do not use personal email accounts for trust business.
- Be polite and appreciate that other users might have different views - the use of strong language, swearing or aggressive behaviour is as anti-social online as it is on the street.
- Emails containing material of a violent, dangerous, racist, or inappropriate content, should be reported to the Safeguarding Officer. The sending or receiving of an email for non-Trust business or containing content unsuitable for education is forbidden.
- Do not open attachments from someone you don't know as they can contain viruses or other programs.

Please read this document carefully. If any of the above are violated you could be subject to disciplinary action and where appropriate, the police may be involved or other legal action taken.

Reporting and dealing with E-safeguarding Incidents



Use of Digital and Video Images

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

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. social networking sites.
- A register will be kept of those students where permission has been obtained from parents to use digital/video images on trust promotional materials including the website. The register will also indicate if a parent has declined such use.
- Staff/trainees may take digital/video images to support the work of the trust. Images should only be taken on trust equipment and the personal equipment of staff should never be used for such purposes.
- Students' full names will not be used anywhere on the trust website particularly in association with photographs.
- Care should be taken when capturing digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the trust into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.

Social Media – Protecting Professional Identity

The trust has a duty of care to provide a safe learning environment for students and staff. The trust could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the trust liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The trust provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the trust through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment including legal risk

Trust staff should ensure that:

- No reference should be made in social media to students, parents, carers or school staff
- They do not engage in online discussion on personal matters relating to members of the trust community
- Personal opinions should not be attributed to the trust
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The Trust's use of social media for professional purposes will be checked regularly by the e-safeguarding committee to ensure compliance with the Social Media, Personal Data, Communications and Use of digital and video images policies.

Personal Data

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

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

Staff/ trainees must ensure that they:

- take care at all times to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices using USB devices provided by the trust.
- delete the data from the device once it has been transferred or its use is complete.
- report the loss of any trust device including laptops and memory sticks immediately

Security

Dedicated security infrastructure allows information systems to be provided a greater level of security than can be achieved by delivering enhanced security capabilities. Without dedicated infrastructure the potential exists that the Trust's information systems could be exploited leading to compromise of information system security. •

- Boundary network access points will be protected by boundary protection systems (a firewall) that monitor and control communications. These systems will be configured to deny external entry by allow or deny exception, to prevent public access to internal networks and to place controls on publicly accessible systems.
- Boundary network access points will be protected by monitoring and/or intrusion prevention systems that monitor events, detect attacks, and provide identification of unauthorized information system use. These systems will be configured to monitor both inbound and outbound communications.

- All information systems will be protected by malware / anti-virus protection systems where such solutions exist for the information system. At a minimum malware protection will be performed at the network boundary, on e-mail and other communications systems, and on all workstations, servers and other endpoints.
- Boundary network access points as well as all information systems will be protected by data protection platforms that monitor, control and restrict the flow of data into and out of systems and into and out of networks. These platforms will include data encryption, session encryption and content filtering.

Passwords

Passwords are the primary form of user authentication used to grant access to the Trust's information systems. To ensure that passwords provide as much security as possible they must be carefully created and used. Without strict usage the potential exists that passwords will be created that are easy to break thus allowing easier access to Trust's information systems, thereby compromising the security of those systems.

- Passwords must be constructed according to set length and complexity requirements. As such passwords must be 6 characters in length and must include 1 upper case and number characters.
- Passwords will have both minimum and maximum lifespan. As such, passwords must be replaced at a maximum of 90 days and at a minimum of 30 days.
- Passwords may not be reused any more frequently than every 5 password refreshes.
- Passwords are to be used and stored in a secure manner. As such, passwords are not to be written down or stored electronically. Passwords are to be obscured during entry into information system login screens.
- Passwords are to be individually owned and kept confidential and are not to be shared under any circumstances.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the trust currently considers the benefits of these technologies for education:

	Staff and other adults				Students			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not Allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to trust	*				*			
Use of mobile phones in lessons		*				*		
Use of mobile phones in social time	*				*			
Taking photos on mobile phones or other personal camera devices				*			*	
Use of personal hand held devices eg PDAs, PSPs		*					*	
Use of personal email addresses in trust, or on trust network				*				*
Use of trust email for personal use				*				*

Use of chat rooms				*				*
Use of instant messaging				*				*
Use of social networking sites				*				*
Use of personal blogs				*				*

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

- The official trust email service is safe, secure and is monitored. Staff and students should therefore only use the trust email service to communicate with others whilst at work.
- Users must immediately report, to any teacher or adult, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students or parents must be professional in tone and content. These communications may only take place on trust systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for such communications.
- Students at KS3 will be provided with internal individual trust email addresses for educational use. Students at KS4 will have monitored, external email access.
- Students will be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the trust website and only official email addresses should be used to identify members of staff

Unsuitable and inappropriate Internet activities

The trust believes that the activities referred to in the following section would be inappropriate in a trust context and that users, as defined below, should not engage in these activities in trust or outside trust when using trust equipment or systems.

The trust policy restricts specific internet usage as follows:		Acceptable at certain times	Acceptable for staff	Unacceptable/Illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images			*
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation			*
	adult material that potentially breaches the Obscene Publications Act in the UK			*
	criminally racist material in UK			*
	pornography			*
	promotion of any kind of discrimination			*
	promotion of racial or religious hatred including radicalisation			*
	threatening behaviour, including promotion of physical violence or mental harm			*
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the trust or brings the trust into disrepute			*

Using trust systems to run a private business			*
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the trust			*
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			*
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet			*
On-line gaming (educational)	*		
On-line gaming (non-educational)	*		
On-line gambling			*
On-line shopping / commerce		*	
File sharing			*
Use of social networking sites		*	
Use of video broadcasting e.g. YouTube		*	

Responding to incidents of misuse

In the event that any apparent or actual misuse appears to involve illegal activity i.e.

- Child sexual abuse images
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Any activity relating to the PREVENT duty
- Other criminal conduct, activity or materials

Then the member of staff should inform the Safeguarding Officer immediately.

Reporting Students

Incident	Teacher to report on SIMS	Study Plus issued	Refer to Safeguarding Officer/System Manager	Interview with student – third recorded incident triggers parent interview	Parent interview	Police informed
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 trust network by sharing username and passwords	*	*				
Attempting to access or accessing the trust network, using another student's account	*		*	*		
Attempting to access or accessing the trust 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	*		*	*		
Actions which could bring the trust into disrepute or breach the integrity of the ethos of the trust	*		*		*	
Using proxy sites or other means to subvert the trust'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	*		*		*	*

Staff disciplinary policy

The following activities are considered inappropriate and will be dealt with in accordance with the trust staff disciplinary policy:

- 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 the trust network by sharing username and passwords or attempting to access or accessing the trust 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 students/students
- Actions which could compromise the staff member's professional standing
- Actions which could bring the trust into disrepute or breach the integrity of the ethos of the trust
- Using proxy sites or other means to subvert the trust'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