Staffordshire University Academies Trust		Trust Policy Document			
Approved by:	**Trust Board**	**Issue date:**	**June 2020**	**Review date:**	**June 2021**
Policy Owner:	**COO**	Page: **1 of 35**			
Audience:	**Trustees** ☑ **Staff** ☑ **Pupils** ☑ **Local Academy Council** ☑ **Parents** ☑ **General Public** ☑				

E- Safety Policy

Purpose

The purpose of this policy is to:

- Ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices
- Provide staff and volunteers with the overarching principles and conduct that guide our approach to online safety
- Ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices and services
- Provide clarity about the use of electronic communications equipment in a manner that is safe and deters users from accessing inappropriate materials
- Promote awareness and to provide guidance to assist staff in providing safeguards to young people in their use of the Internet and other forms of Information Communications Technology
- Safeguard pupils and staff in using online platforms

Schedule for Development / Monitoring / Review

The E-Safety Policy was approved by the SUAT Trust Board*:*	Delegated to COO 6/3/2015
The implementation of this e-safety policy will be monitored by the:	Individual Academies Local Academy Councils SUAT SUAT Trust Board
Monitoring will take place at regular intervals:	Six monthly
The Local Academy Council members will receive a report on the implementation of the e-safety policy generated by each Academy at regular intervals:	Within safeguarding reports to the Local Academy Council
The E-Safety 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-safety or incidents that have taken place. The next anticipated review date will be:	Annually (June 2021)
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	Local Children Services / Staffordshire Safeguarding Children's Board / Police / NSPCC / MASH / Social Workers (as relevant

Academies will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)

- Internal monitoring data for network activity
- Staff meetings and parental feedback forums
- Online safety training
- Where necessary, surveys / questionnaires of:
  - pupils
  - parents / carers
  - staff

Scope of the Policy

Government guidance across the UK highlights the importance of safeguarding children and young people from harmful and inappropriate online material (Department for Education, 2019a). All adults who come into contact with children and young people in their work have a duty of care to safeguard and promote their welfare. (1989 Children Act and Child Care Act 2000). The Children Act 2004 places a duty on organisations to safeguard and promote the well-being of children and young people; this encompasses e-safety.

A whole school approach to online safety helps ensure staff, Local Academy Council members, volunteers and parents teach children about online safety, because the internet and online technology provides so many new opportunities for young people's learning and growth, but it can also expose them to new types of risks. The Education and Inspections Act 2006 empowers Principals/Head Teachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying and e-safety incidents covered by this policy, which may take place outside of an Academy. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

Having an online presence is now an integral part of children and young people's lives. Social media, online games, websites and apps can be accessed through mobile phones, computers, laptops and tablets – all of which form a part of children and young people's online environment, therefore, e-safety should form a fundamental part of safeguarding and child protection measures and procedures.

This policy applies to all members of SUAT's community (including staff, pupils, volunteers, parents / carers, members of the Trust Board, members of the Local Academy Councils, visitors, community users) who have access to and are users of SUAT and Academy ICT systems, both in and out of the educational setting.

SUAT and the Academies will deal with e-safety incidents and associated behaviour in a manner which is proportionate to the incident, to ensure that pupils learn in a supportive, caring and safe environment without fear of bullying and online safety threats, and to defend the right of every child and adult to be happy and secure inside and outside of the educational environment.

Roles and Responsibilities

The Trust Board and Local Academy Councils

The Trust Board are responsible for the approval of the E-Safety Policy.

Reviewing the effectiveness of the policy will be the responsibility of individual Academies and their safeguarding leads, supported by Local Academy Council members after receiving regular information about E-Safety incidents and monitoring reports. A member of the Local Academy Council will support each Academy with E-Safety, including:

- Meetings with the E-Safety Coordinator.
- Regular monitoring of E-Safety incident logs.
- Monitoring of filtering / change control logs.
- Reporting back to the Local Academy Council.

Principal / Head Teacher and Senior Leaders

- The Principal / Head Teacher has a duty of care for ensuring the safety (including e-safety) of members of their Academy community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator.
- The Principal and the Senior Leadership Team 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 Principal and Senior Leaders are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, to the appropriate level, according to their job role.
- The Principal and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in their Academy who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Coordinator and be made immediately aware of a safeguarding issue.
- The Principal and Senior Leaders will be responsible for ensuring that staff are appropriately trained in e-safety and understand the procedures they must follow to a) help mitigate incidents and b) report and manage incidents should they arise.

E-Safety Coordinator / Safeguarding Officer

Should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

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

- Cyber-bullying.

Key responsibilities include:

- Leading Academy E-Safety.
- Taking day to day responsibility for E-Safety issues and being a leading role in establishing and reviewing the E-Safety policies, procedures and documents in conjunction with the Senior Leadership Team.
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Providing training and advice for staff.
- Liaising with SUAT/Academy technical staff.
- Receiving reports of E-Safety incidents and creates a log of incidents to inform future E-Safety developments.
- Meeting with the Senior Leadership Team to discuss current issues, review incident logs and filtering / change control logs.
- Report to the Local Academy Council regarding current issues, review incident logs and filtering / change control logs.
- Reporting regularly to the Senior Leadership Team.

ICT Manager / ICT Support Team
The ICT Manager / ICT Support Team is responsible for ensuring:

- That the Trust's and each Academy's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the academies meet required e-safety technical requirements.
- That users may only access the networks and devices through a properly enforced password protection in which passwords are regularly changed (at least termly).
- The filtering policy is applied, assessed for suitability and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- Requests to amend filtering policy, such as unblocking uncategorised websites, are carefully reviewed before approving (approval for unblocking sites should be provided by the Principal / Head Teacher where relevant).
- The firewall is functional and incorporates appropriate security rules to prevent a compromise to the network.
- That they keep up to date with E-Safety technical information in order to effectively carry out their E-Safety role and to inform and update others as relevant.
- That the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Coordinator for investigation / action / sanction.
- That monitoring software / systems are implemented and updated as agreed in this policy.
- Will ensure where appropriate academy owned classroom based mobile devices are properly locked down to ensure there is no misuse of cameras or online platforms such as unauthorsed websites, social media, personal emails etc.
- Servers, wireless systems and cabling must be securely located and physical access restricted

Teaching and Support Staff
Are responsible for ensuring that:

- They have an up to date awareness of E-Safety matters and of the current SUAT and Academy E-Safety policy and practices.
- They have read, understood and signed the Staff Acceptable Use Policy and code of conduct.
- They report any suspected misuse or problem to the E-Safety Coordinator / Designated Safeguarding Lead for investigation / action / sanction, immediately, or as soon as possible following the incident, depending on the nature and severity of the incident.
- All digital communications with pupils / parents / carers should be on a professional level and only carried out using official Academy systems in accordance with SUAT Data Protection Policies.
- E-Safety issues are embedded in all aspects of the curriculum and other activities.
- Pupils understand and follow the E-Safety and acceptable use policies.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other activities (where allowed) and implement current policies with regard to these devices.
- In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Pupils

- Are responsible for using Academy digital technology systems in accordance with the Pupil Acceptable Use Policy
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulation (where relevant)
- 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 policies on the use of Academy approved mobile devices and digital cameras. They should also understand procedures in relation to the taking and use of images and cyber-bullying. Pupils will be taught about E-Safety according to their age group and ability to understand, in a format which they will be able understand.
- Should understand the importance of adopting good e-safety practice when using digital technologies outside of the Academies.

Parents / Carers
Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. SUAT Academies will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local E-Safety campaigns / literature. Parents and carers will be encouraged to support the Academies in promoting good E-Safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at events (and in accordance with the Use of Images Policy)
- Access to parents' sections of the website / VLE and online pupil records

- Their children's personal devices in the SUAT academies
- Social media platforms (in accordance with the Social Media Policy)
- Safe use of online platforms and data sharing

Community Users
Community Users who access SUAT and Academy systems / website / VLE as part of the wider Academy provision will be expected to sign a Community User Acceptable Use Agreement before being provided with access to SUAT systems**.** The Academies will ensure that appropriate security measures are implemented before any members of the community and visitors are permitted access to online environments using SUAT / Academy ICT systems (inclusive of Wi-Fi).

Education and Training

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

E-safety should be a focus of the curriculum and staff should reinforce E-Safety messages across the curriculum. The E-Safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided by::

- A planned e-safety curriculum should be provided as part of the curriculum and should be regularly revisited
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities, where relevant
- Pupils should be taught to be critically aware of the materials / content they access online and be guided to validate the accuracy of information
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet (where relevant)
- Pupils should be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside of SUAT academies
- Staff should act as good role models in their use of digital technologies on the internet and mobile devices
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. N.B. additional duties for schools/academies under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.
- In lessons where internet use is pre-planned, it is best practice that students/pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students/pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents / Carers

Many parents and carers may only have a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. The frequency to which children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond should not be underestimated.

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

- Curriculum activities
- Letters, newsletters, web site
- Parents / carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g.

Childnet
Think u know
NSPCC
Safer Internet

Education & Training – Staff and Volunteers

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

- A planned programme of formal E-Safety training will be provided for Academy staff by the Academy. This will be regularly updated and reinforced. An audit of the E-Safety training needs of all staff will be carried out regularly by each Academy
- All new staff should receive E-Safety training as part of their induction programme, ensuring that they fully understand the SUAT E-Safety Policy and Acceptable Use Agreements
- The E-Safety Coordinator will receive regular updates through attendance at external training events (e.g. from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations
- The E-Safety Coordinator will provide advice / guidance / training to individuals as required. Trustees and Local Academy Council members are invited to take part in E-Safety training and awareness sessions, with particular importance for those who are members of any committee or working group involved in technology, E-Safety, health and safety or child protection
- This online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions.

- It is expected that some staff will identify online safety as a training need within the performance management process.

Technical – Infrastructure / Equipment

Each Academy will be responsible for ensuring that their infrastructure is as safe and secure as far as is reasonably practicable and that E-Safety policies and procedures are implemented. It will also ensure that those involved in implementing, supporting and managing E-Safety will be effective in carrying out their responsibilities:

- SUAT technical systems will be managed in ways that ensure they meet recommended security, safeguarding and prevent requirements
- There will be regular reviews and audits of the safety and security of SUAT technical systems by ICT staff and providers to ensure adequacy
- Servers, wireless systems and cabling must be securely located and physical access restricted to authorised staff only
- All users will have clearly defined access rights to SUAT technical systems and devices, as approved by the Principal / Head Teacher
- Software licence logs are accurate and up to date and regular checks are made to reconcile the number of licences purchased against the number of software installations
- Appropriate security measures are in place to protect the servers, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the SUAT systems and data. These are tested regularly and are monitored continually by IT staff and Management Providers. Potential security threats are reported to the Head Teacher/Principal and where necessary in accordance with data protection procedures, the DPO.
- The SUAT IT infrastructure and individual workstations are protected by up to date anti-virus software, safeguard filtering systems, critical/security updates, firewalls and policies such as regular password renewal~~, password protection.~~.
- School approved USB and storage devices are only to used with school systems.

Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be Academy owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising Academy wireless network. The device then has access to the wider internet which may include Academy learning platforms and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. The use of mobile technologies should be consistent with and inter-related to other relevant school polices including but not limited to the safeguarding policy, behaviour policy, anti-bullying policy, acceptable use policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of Academy online safety education programme.

The possible issues and risks of BYOD/BYOT may include:

- Security risks in allowing connections to Academy networks
- Filtering of personal devices
- Breakages and insurance
- Access to devices for all pupils
- Avoiding potential classroom distraction
- Network connection speeds
- Types of devices
- Charging facilities and electrical compliance
- Total cost of ownership.
- Incompatibility with school systems
- Data loss
- School systems may enforce admin rights over devices and amend device settings

Aspects that each Academy should consider and be included in their online safety policy, mobile technologies policy or acceptable use agreements area:

Academy owned/provided devices:

- Who they will be allocated to
- Where, when and how their use is allowed – times/places/in school/out of school
- If personal use is allowed
- Levels of access to networks/internet (as above)
- Management of devices/installation of apps/changing of settings/monitoring
- Network/broadband capacity
- Technical support
- Filtering of devices
- Access to cloud services
- Data Protection
- Taking/storage/use of images
- Exit processes – what happens to devices/software/apps/stored data if user leaves the school
- Liability for damage
- Staff training

Personal devices:

- Which users are allowed to use personal mobile devices in school (staff/pupils/students/visitors)
- Restrictions on where, when and how they may be used in school
- Storage
- Whether staff will be allowed to use personal devices for school business
- Levels of access to networks/internet (as above)
- Network/broadband capacity
- Technical support (this may be a clear statement that no technical support is available)
- Filtering of the internet connection to these devices
- Data Protection

- The right to take, examine and search users devices in the case of misuse (England only) – N.B. this must also be included in the Behaviour Policy.
- Taking/storage/use of images
- Liability for loss/damage or malfunction following access to the network (likely to be a disclaimer about school responsibility).
- Identification/labelling of personal devices
- How visitors will be informed about school requirements
- How education about the safe and responsible use of mobile devices is included in the school online safety education programmes.

When personal data is stored on any mobile device or removable media the:

- Data must be encrypted and password protected
- Device must be password protected; (be sure to select devices that can be protected in this way)
- Device must be protected by up to date virus and malware checking software
- Data must be securely deleted from the device, in line with Academy policy once it has been transferred or its use is complete.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Can recognise a possible breach, understand the need for urgency and know who to report it to within the Academy, who will escalate potential breaches to the DPO upon immediately becoming aware of the issue
- Can help data subjects understands their rights and know how to handle a request whether verbal or written. Know who to pass it to in the Academy
- Where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected.
- Will not transfer any school/academy personal data to personal devices except as in line with Academy policy
- Access personal data sources and records 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
- Do not take academy devices off site without permission of the Head Teacher / Principal

Filtering & Monitoring

~~SUAT recognises that no filter can guarantee to be 100% effective but~~ Academies should be satisfied that their filtering system is effective in categorising the ~~manages the~~ following content online and on their systems~~(and web search)~~ and appropriate reporting is available for violations:

- Discrimination: Promotes the unjust or prejudicial treatment of people on the grounds of the protected characteristics listed in the Equality Act 2010
- Drugs / Substance abuse: displays or promotes the illegal use of drugs or substances
- Extremism: promotes terrorism and terrorist ideologies, violence or intolerance
- Malware / Hacking: promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content
- Pornography: displays sexual acts or explicit images
- Piracy and copyright theft: includes illegal provision of copyrighted material
- Self Harm: promotes or displays deliberate self harm (including suicide and eating disorders)
- Violence: Displays or promotes the use of physical force intended to hurt or kill
- Gambling
- Any malicious, harmful or inappropriate content

Access to illegal content must be blocked, specifically that the filtering providers: are IWF members and block access to illegal Child Sexual Abuse Material (CSAM) and integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office.'

Academies should consider that their filtering system meets the following principles:

- Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and ability to understand the complexities of internet content
- Circumvention – the extent and ability to identify and manage technologies and techniques used to circumvent the system, for example VPN, proxy services and DNS over HTTPS
- Control - has the ability and ease of use that allows the Academy to control the filter themselves to permit or deny access to specific content
- Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking. Each Academy should have access to their filtering policy
- Group/Multi-site Management – the ability for deployment of central policy and central oversight or dashboard
- Identification - the filtering system should have the ability to identify users
- Mobile and App content – mobile and app content is often delivered in entirely different mechanisms from that delivered through a traditional web browser. The filter system must also block inappropriate content via mobile and app technologies (beyond typical web browser delivered content). Where mobile devices are taken off the school infrastructure or fall outside of this filtering, then other appropriate device level filtering will be in place to ensure safeguarding (such as Mobile Device Management tools)
- Multiple language support – the ability for the system to manage relevant languages
- Reporting mechanism – the ability to report inappropriate content for access or blocking
- Reports – the system offers clear historical information on the websites visited by Academy users

All use of Academy internet access is logged and the logs are regularly monitored by IT support or designated safeguarding leads. Whenever any inappropriate use is detected it will be followed up by the E-Safety Coordinator, DSL or member of the Senior Leadership Team depending on the severity of the incident.

Each Academy will have monitoring software in place for every device (including laptops, mobile devices and desktops) which detects potentially inappropriate content and conduct as soon as it appears on the screen, is typed in by any users or received by the user. A capture is taken of every incident detailing the time and date of capture, machine name, username and reason for capture. SUAT recognises that some captures will be false positives however, where it has been established that the capture is a violation, this will be investigated and dealt with in accordance to the AUP, behaviour policy and other relevant SUAT policies. The E-Safety Coordinator/IT Support will maintain the Change Control Log and record any breaches, suspected or actual, of the filtering and security systems. Breaches which result in the potential personal data breaches will be reported to the DPO for investigation immediately.

Any member of staff employed by the SUAT who comes across an e-safety issue does not investigate any further but immediately reports it to the E-Safety Coordinator, designated safeguarding lead or Principal/Head Teacher and impounds the equipment. This is part of the SUAT safeguarding protocol.

Although remote monitoring is in place on all SUAT devices to flag potential areas of concern and breaches, the monitoring of E-Safety in each individual academy will take many different forms. This includes:

Physical Monitoring
Most suited where circumstances and the assessment suggests low risk. This could be:

- Physical supervision of children while using the internet;
- Assigning additional classroom support staff to monitor screen activity;
- Or actively monitoring all screen activity during a lesson from a central console using appropriate technology.

The following are possible limitations and points to consider:

- Can be resource intensive
- Less effective across a larger group or a group using mobile devices
- Screen behaviour can be adapted to avoid monitoring
- Advantage of immediate intervention when an issue arises which can be developed as a teaching opportunity

Internet and web access
Some Internet Service Providers (ISPs), filtering providers or monitoring software provide logfile and regular reports, providing information of details and attributes website access and search term usage against individuals. Through regular monitoring, this information could enable Academies to identify and intervene with issues concerning access or searches.

The following are possible limitations and points to consider:

- Assign appropriate responsibility for analysing this information. These reports can often be difficult to understand and may require support to analyse
- The frequency that block or monitoring lists are updated

- The information should be able to identify an individual user (or group as appropriate) for effective intervention
- Logs need to be regularly reviewed, interpreted and alerts prioritised for intervention
- Information held by the Academy that indicates potential harm, must be acted upon
- Awareness of any limitations of the information reported

Monitoring Strategy/System Features

Academies consider how their system integrates within their policies and should satisfy themselves that their monitoring strategy meets the following principles:

- Age appropriate – includes the ability to implement variable monitoring appropriate to age. This will in turn define which alerts are prioritised and responded to.
- BYOD (Bring Your Own Device) – if the system includes the capability to monitor personal mobile and app technologies (i.e. not owned by the Academy), decide what the device will be used for and how appropriate monitoring will be deployed and managed. Monitoring must not take place outside of academy hours for data protection purposes. The DPO must be consulted where this option is available to staff and pupils.
- Data retention – the Compliant Records Management Policy details what data is stored, where, for how long and how it should be securely disposed of.
- Devices – the software monitoring system should be clear about the devices (and operating systems) it covers.
- Flexibility - changes in keywords (addition or subtraction) can be easily amended according to an agreed policy.
- Group management – the ability for deployment of central policy and central oversight or dashboard.
- Impact - monitoring results must inform Academy policy and practice reviews and permit the development and improvement of e-safety practice.
- Monitoring Policy – all users must be made aware that their activities are being monitored via the acceptable use agreement / policy. Expectations of appropriate use are communicated and agreed through this format.
- Multiple language support – the ability for the system to manage relevant languages where required.
- Prioritisation – alerts generated via monitoring are prioritised to enable a rapid response to immediate issues.
- Reporting – alerts which are not false must be recorded (in a secure format), reported to the Principal / DSL / E-Safety Coordinator, investigated and dealt with.

Password Security

- All users will have clearly defined access rights to SUAT and Academy technical systems and devices, this will be reviewed, at least annually, by the Academy with support from their IT Team or IT Support Provider
- All SUAT networks and systems will be protected by secure passwords that are regularly changed (at least termly). Service accounts required for 3rd party integration or automation purposes (not used by members of staff) that are not able to change without causing disruption

to daily productivity, will be secured with a highly complex password of 16 characters including capitals and special characters.

- The "master / administrator" passwords for the SUAT systems, used by the technical staff must also be available to the academy Principals/Head Teachers or other nominated senior leader and kept in a secure place which is not accessible to unauthorised users, at all times
- Passwords for new users, and replacement passwords for existing users will be allocated by IT Support
- All users (adults and young people) will have responsibility for the security of their username and password, they must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- Users will change their passwords at regular intervals (at least termly) – as described in the staff and pupil sections below
- Passwords will be of appropriate length and complexity i.e. at least eight characters of mixed characters.

Staff Passwords

- All staff users will be provided with a username and password by their IT Support who will keep an up to date record of users and their usernames
- The password should be a minimum of 8 characters long and must include at least one of – uppercase character, number, special characters
- Passwords must not include proper names or any other personal information about the user that might be known by others
- The account should be "locked out" following three successive incorrect log-on attempts
- Temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on
- Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of SUAT academies
- Passwords must be changed at least every term
- Passwords should not be re-used for 6 months and be significantly different from previous passwords
- Passwords must be kept secure at all times, not be shared and be inaccessible to others

Pupil Passwords

- All users will be provided with a username and password by IT Support who will keep an up to date record of users and their usernames
- Pupils will be taught the importance of password security
- The complexity (i.e. minimum standards) will be set with regards to the cognitive ability of the children

Incident Reporting

If any e-safety events or online abuse occurs, the Academy will respond to this by:

- Immediately reporting to the Principal (if a member of staff) or the DSL / E-Safety Coordinator (if a pupil) who will investigate further following e-safety and safeguarding policies and guidance.

- Following the Academy's clear and robust safeguarding procedures in place for responding to abuse (including online abuse) as detailed within the Safeguarding Policy
- Providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying/cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation as required
- Making sure the response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account
- Reviewing the policies and procedures developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term

Responding to incidents of misuse

It is hoped that all members of the SUAT community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place through careless or irresponsible, or very rarely, through deliberate misuse. Listed in Appendix 2 are the responses that will be made to any apparent or actual incidents of misuse.

If any apparent or actual, misuse appears to involve illegal activity e.g. child sexual abuse images, adult material which potentially breaches the Obscene Publications Act, criminally racist material or other criminal conduct, activity or materials the flow chart should be consulted. Actions will be followed in accordance with policy, in particular the sections on reporting the incident to the police and the preservation of evidence. If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is recommended that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer.

It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of SUAT's community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows (Appendix 3 for pupils and Appendix 4 for staff respectively).

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below).

- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by the Trust or national/local organisation (as relevant).
    - Police involvement and/or action
    - HR consultation
- **If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - offences under the Computer Misuse Act (see User Actions chart above)
    - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the Academy/Trust and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

Use of digital and video images

- The individual academies record of parental permissions granted/not granted must be adhered to when taking images of our pupils. A list is published to all staff on a termly basis, but can also be obtained from the designated person who manages permissions in the individual Academies
- Under no circumstances should images be taken using privately owned equipment.
- Where permission is granted the images should be transferred to individual academy storage systems (server or disc) and deleted from privately owned equipment at the earliest opportunity
- Permission to use images of all staff who work for SUAT is sought on induction and a copy is located in the personnel file
- The Use of Images Policy must be consulted and referred to for the use of both photographic and video images of staff and pupils

Although many of the above points are preventative and safeguarding measures, it should be noted that SUAT will endeavour whenever possible to use social networking in positive ways to publicise, inform and communicate information. SUAT and individual academies have active websites, and may have social media pages such as Facebook and Twitter accounts which are used to inform, publicise events and celebrate and share the achievement of pupils.

When using communication technologies, the following conduct is required:

- The official academy email system may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the Academy email system to communicate with others

when in school, or on SUAT systems (e.g. by remote access), provided that this is undertaken in compliance with data protection policies.

- Users need to be aware that email communications may be monitored.
- Users must immediately report, to the nominated person, 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 pupils or parents/carers (email, chat, etc.) must be professional in tone and content. These communications may only take place on official (monitored) academy systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications
- Pupils should 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 SUAT websites and only official email addresses should be used to identify members of staff, where it is necessary that their information is published.
- Only designated personnel may publish on academy social media and online platforms.
- Appropriate written consent must be in place before making any online publications involving personal information.
- The person utilising the system is responsible for ensuring that their actions adhere to data protection policies and maintain the security and protection of personal information of themselves and others.

Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school/academy and the individual when publishing any material online. Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'. Ofsted's online safety inspection framework reviews how a school/academy protects and educates staff and pupils in their use of technology, including the measures that would be expected to be in place to intervene and support should a particular issue arise. Schools/academies are increasingly using social media as a powerful learning tool and means of communication. It is important that this is carried out in a safe and responsible way.

The Academy/Trust provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and Academies through:

- Ensuring that personal information is not published
- Training is provided including: 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

Academy/Trust staff should ensure that:

- No reference should be made in social media to students/pupils, parents/carers or Academy staff

- They do not engage in online discussion on personal matters relating to members of the Academy community
- Personal opinions should not be attributed to the Academy or Trust
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official Academy social media accounts are established there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including systems for reporting and dealing with abuse and misuse and an understanding of how incidents may be dealt with under Academy disciplinary procedures

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the Academy/Trust or impacts on the Academy/Trust, it must be made clear that the member of staff is not communicating on behalf of the Academy/Trust with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the Academy/Trust are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The Academy permits reasonable and appropriate access to private social media sites

Monitoring of Public Social Media:

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about each Academy
- Each Academy should effectively respond to social media comments made by others according to their defined policy or process

Each Academy's use of social media for professional purposes will be checked regularly by the Senior Leadership Team and E-Safety Coordinator to ensure compliance with the relevant policies.

Loaning Devices

Academies loaning devices to staff / pupils must ensure:

- That the device has appropriate security measures such as encryption, filtering software, antivirus installed
- The device is capable of monitoring activity

- There is a written agreement in place with the individual, which details the period of the loan, conditions of loaning the device, that the device should be returned to the Academy in the same physical and technical condition it was loaned in
- The individual has signed the relevant acceptable use and loan agreement
- No alterations are made to the technical specification or makeup of the device
- The loan is recorded on the relevant asset register
- Terms are in place to maintain the security of the device whilst off site, and the user understands and has agreed to these terms

Appendix 1

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the academy currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

		Staff and other adults					Pupils and young people			
Communication Technologies		Permitted	Permitted at certain times	Permitted for named staff	Not Permitted		Permitted	Permitted at certain times	Allowed with staff permission	Not Permitted
Mobile phones may be brought to the academy		☑								☑
Mobile phones used in lessons					☑					☑
Use of mobile phones in social time, in designated 'mobile phone areas'		☑								☑
Taking photographs on mobile devices					☑					☑
Use of academy mobile devices		☑								☑
Use of Academy email for personal emails					☑					☑
Use of personal social network sites during break times			☑							☑
Use of academy social media platforms and website		☑								☑
Use of educational blogs		☑							☑	

Appendix 2

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material are illegal and is banned from all SUAT ICT systems. Other activities e.g. Cyber-bullying is banned and could lead to criminal prosecution.

There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities. SUAT believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in the work/education or outside when using SUAT equipment or systems. 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 SUAT policy restricts certain internet usage as follows:

User actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Child sexual abuse images contrary to the Protection of Children Act 1978					□
Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					□
Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					□
Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					□
Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					□
Promotion or conduct of illegal acts, e.g. 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 the UK					□
Pornography					□
Promotion of any kind of discrimination				□	
Promotion of racial or religious hatred				□	
Threatening behaviour, including promotion of physical violence or mental harm				□	
Any other information which is not illegal but may be offensive to colleagues or breaches the integrity of the ethos of the SUAT academies or brings a SUAT academy into disrepute				□	
Using academy systems to run a private business				□	
Use systems, applications, websites or other				□	

mechanisms that bypass the filtering or other safeguards employed by BMBC and / or the academy					
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				□	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)					□
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			□		
Downloading video broadcasting e.g. Youtube			□		
Uploading to video broadcast e.g. Youtube with appropriate permissions			□		

Appendix 3

Incident involving pupils	Teacher to use academy behaviour policy to deal with	Refer to Principal/SLT – Liaise with Safeguarding Officer as appropriate	Refer to police	Refer to technical support staff for action re security/filtering etc.
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 (those whereby the content is legal)	□			□
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 (those whereby the content is legal)		□		□
Allowing others to access SUAT academies network by sharing username and passwords		□		□
Attempting to access or accessing SUAT academies' networks, using another pupil's account		□		□
Attempting to access or accessing the SUAT academies 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		□	Community Police Officer referral	□
Actions which could bring the Academy into disrepute or breach the integrity of the ethos of SUAT		□		□
Using proxy sites or other means to subvert the filtering system		□		□
Accidentally accessing offensive or pornographic material and failing to report the incident		□		□

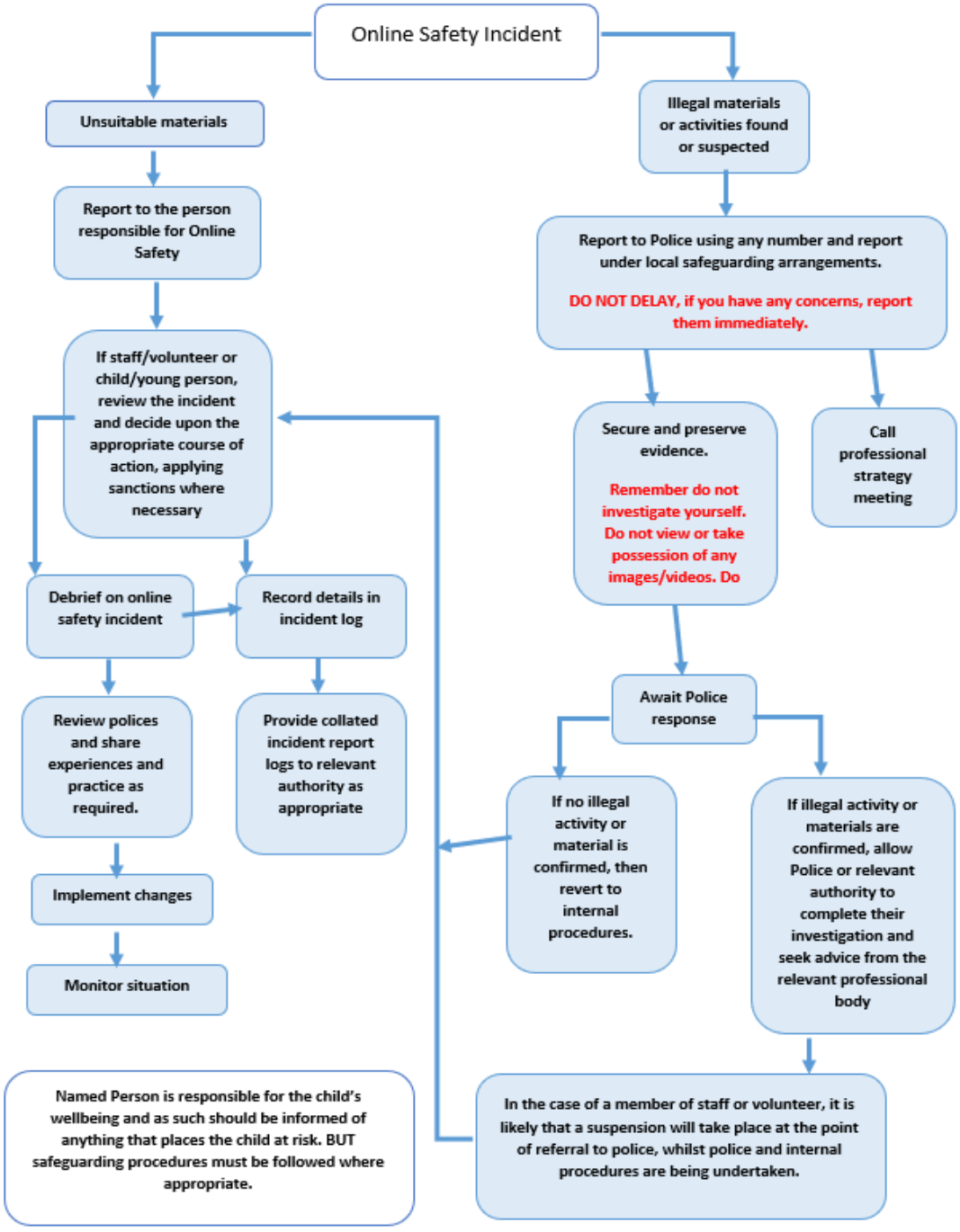
Appendix 4

Incidents involving members of staff	**Refer to the Principal**	**Refer to technical support staff for action re filtering, security etc.**	**Potential Disciplinary Action**
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable /inappropriate activities).	☐	☐	☐
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	☐		☐
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 SUAT academies network by sharing username and passwords or attempting to access or accessing the 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	☐	☐	☐
Actions which could compromise the staff member's professional standing	☐		☐
Actions which could bring the SUAT academies into disrepute or breach the integrity of the ethos of the SUAT	☐		☐
Using proxy sites or other means to subvert the SUAT academies filtering system	☐	☐	☐
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	☐		☐

Appendix 5

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Appendix 6

Student Acceptable Use Agreement

Academy Policy
Digital technologies have become integral to the lives of children and young people, both within the Academy and outside. These 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 and these digital technologies.

This Acceptable Use Policy is intended to ensure:
- All end users will be responsible and stay safe while using the internet and other digital technologies for educational, personal and recreational use
- That SUAT and Academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk

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

Acceptable Use Policy Agreement
I understand that I must use Academy ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:
- I understand that the Academy will monitor my use of the systems, devices and digital communications
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it
- I will be aware of "stranger danger" when I am communicating online
- I will not disclose or share personal information about myself or others when online (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If someone I have communicated with online has asked to meet in person, I will inform a responsible adult (parent/carer/teacher) before meeting this person
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online

I understand that everyone has equal rights to use technology as a resource and:
- I understand that the SUAT systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work
- I will not use the SUAT systems or devices for online gaming, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so

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

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

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

- I will only use my own personal devices (mobile phones / USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in the Academy, I will follow the rules set out in this agreement, in the same way as if I was using Academy equipment. I will ensure that all files are checked for viruses
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials
- I will immediately report any damage or faults involving equipment or software, however this may have happened
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any Academy device, nor will I try to alter computer settings
- I will only use social media sites with permission and at the times that are allowed

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

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

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

- I understand that the Academy also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of the Academy and where they involve my membership of SUAT's community (examples would be cyber-bullying, use of images or personal information)
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the Academy network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to Academy systems and devices.

Student Acceptable Use Agreement Form

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

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

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

Name of Student	
Tutor Group	
Signature	
Date	

Appendix 6

Pupil Acceptable Use Policy Agreement – for younger pupils

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer

Name of child: ……

Date read and explained to child: ……...

Signed (parent): ……..

Appendix 7

Staff (and Volunteer) ICT Acceptable Use Policy Agreement

New technologies have become integral to the lives of children and young people in today's society, both within Academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies.

This Acceptable Use Policy is intended to ensure:

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

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

Acceptable Use Agreement

I understand that I must use Academy ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the Academy may monitor my use of the ICT systems, email and other digital communications
- I understand that the rules set out in this agreement also apply to use of Academy ICT systems (e.g. laptops, email etc.) outside of the school, and to the transfer of personal data (digital or paper based) out of the Academy
- I understand that Academy ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the Trust and Academy
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may gain access to it
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person (Principal or Senior leadership team member with ICT responsibility)

Use of social media

SUAT staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or SUAT staff that is perceived to be slanderous
- They do not engage in online discussion on personal matters relating to members of the Trust's or Academy's community, other schools, the Trust sponsor, or connected organisations
- Personal opinions should not be attributed to SUAT or an individual academy
- They check their security settings on personal social media profiles regularly to minimise risk of loss of personal information
- They are aware of their role within the community and the position of trust they are in, therefore careful consideration should be given to any material that is posted on the internet and social media environments
- They do not invite ex-pupils to be online friends / have access to social media environments they contribute to
- They have checked privacy settings on all of their social media presence
- They are aware that when they respond to Academy social media sites their personal information may be available if the appropriate security / privacy settings have not been set up correctly

I will be professional in my communications and actions when using SUAT ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with SUAT's policy on the use of digital / video images. I will not use my personal equipment to record these images. Where these images are published on SUAT or Academy websites or social media it will not be possible to identify by name, or other personal information, those who are featured
- I will not use personal chat and social media networking sites in the academy unless this is in line with work within the Trust. Please speak to the Principal if in doubt
- I will only communicate with pupils and parents / carers using official Academy systems; all communication will be professional in tone and manner
- I will not engage in any on-line activity that may compromise my professional responsibilities or compromise the reputation of the sponsor, SUAT or any individual academy

The Academy has a responsibility to provide safe and secure access to technologies:

- When I use my personal mobile devices (laptops / mobile phones / USB devices etc.) in the Academy, I will follow the rules set out in this agreement, in the same way as if I was using Academy equipment. I will also follow any additional rules set by the Academy about such use. I will ensure that any such devices are protected by up to date anti-virus software and regularly scanned so they are free from viruses. I will not use personal email addresses for Academy work or on their ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)

- I will ensure that any data not stored on the Academy network is regularly backed up onto my OneDrive area (or other system for back ups).
- I will not upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others. I will not willingly use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not (unless I have permission from the Principal) make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless agreed with the Principal.
- I will not disable or cause any damage to Academy equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the SUAT Data Protection Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based protected and restricted data must be held in lockable storage.
- When using USB sticks / external hard drives I will ensure that all data that may contain personal information is encrypted and not accessible by others
- I understand the SUAT Data Protection Policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by SUAT policy to disclose such information to an appropriate authority. I understand that this must be undertaken securely
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for SUAT sanctioned personal use:

- I will ensure that I have permission to use the original work of others' in my own work.
- Where work is protected by copyright, I will not download or distribute copies.
- If using audio / visual material during lessons, I will ensure that the age restriction is appropriate for the audience (i.e. do not show 15 certificate films to Year 7 pupils). If I wish to show material that is of a different age restriction then parental consent will be sought.

Please read the 'Additional Department for Education Guidance' document for the latest guidance.

I understand that I am responsible for my conduct whilst using ICT in and out of the Academy

- I understand that this Acceptable Use Policy applies not only to my work and use of Academy ICT equipment, but also applies to my use of ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by SUAT
- I understand that if I breach fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action in line with SUAT policies

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

Staff / Volunteer Name

Signed

Date

Appendix 8

Parent / Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within the Academy and outside. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access and access to digital technologies.

This Acceptable Use Policy is intended to 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 Academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- That parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their online behaviour

The Academy will try to ensure that *pupils* will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of Academy expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the Academy in this important aspect of the it's work.

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the Trust or individual academy website and occasionally in the public media.

SUAT academies will comply with the Data Protection Act and request parents / carers permission before taking images of pupils or staff, in accordance with our Use of Images Policy. We will also

ensure that when images are published that the young people cannot be identified by the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the Academy will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the Academy cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the Academy will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the Academy if I have concerns over my child's E-Safety.

As the parent / carer of the above pupils, I give permission for my son / daughter to have access to the internet and to ICT systems at school.	Yes / No
I agree that if I take digital or video images at, or of school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.	Yes / No

Signed

Date

Appendix 9

Acceptable Use Agreement for Community

This Acceptable Use Agreement is intended to ensure:

- that community users of Academy digital technologies will be responsible users and stay safe while using these systems and devices
- that Academy systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- that users are protected from potential risk in their use of these systems and devices

Acceptable Use Agreement

I understand that I must use Academy systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into SUAT academies.

- I understand that my use of Academy systems and devices and digital communications will be monitored
- I will not use a personal device that I have brought into the Academy for any activity that would be inappropriate in a school setting
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person
- I will not access, copy, remove or otherwise alter any other user's files, without permission
- I will ensure that if I take and / or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images. If images are published it will not be possible to identify by name, or other personal information, those who are featured
- I will not publish or share any information I have obtained whilst in the Academy on any personal website, social networking site or through any other means, unless I have permission from the individual Academy
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work
- I will not install or attempt to install programmes of any type on an Academy device, nor will I try to alter computer settings, unless I have permission to do so
- I will not disable or cause any damage to SUAT equipment, or the equipment belonging to others
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos)
- I understand that if I fail to comply with this Acceptable Use Agreement, the Academy has the right to remove my access to Academy systems / devices

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

Name

Signed

Date